

BEFORE THE
Federal Communications Commission
WASHINGTON, D.C. 20554

In the Matter of)	
)	
Continental Airlines of Houston, Texas)	ET Docket No. 05-247
)	
Petition for Declaratory Ruling Regarding)	
Whether Certain Restrictions on Antenna)	
Installation Are Permissible Under the)	
Commission's Over-the-Air Reception Devices)	
(OTARD) Rules)	
 To: The Office of Engineering and Technology		

COMMENTS OF THE MASSACHUSETTS PORT AUTHORITY

By: Christine M. Gill
Keith A. McCrickard
McDERMOTT WILL & EMERY LLP
600 Thirteenth Street, N.W.
Washington, D.C. 20005-3096
202.756.8000

David S. Mackey
Deborah Lau Kee
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
617.568.3131

Its Attorneys

Dated: September 28, 2005

TABLE OF CONTENTS

	Page
I. INTRODUCTION.....	2
II. BACKGROUND.....	4
A. The Massachusetts Port Authority.....	4
1. Management Responsibilities.....	4
2. Size and Scope of Airport Facilities.....	6
3. Leasing Arrangements.....	8
B. Description of Central Wi-Fi Antenna System	11
C. Interference.....	20
III. APPLICABLE LAW AND STANDARD OF REVIEW.....	25
IV. THE EXISTENCE OF A CENTRAL ANTENNA SYSTEM PERMITS MASSPORT TO RESTRICT THE INSTALLATION AND USE OF CONTINENTAL'S ANTENNA	27
A. Continental Would Have Access to Its Desired Service and Desired Service Provider	29
1. Continental Employees.....	29
2. Preferential Passengers.....	31
B. The Central Wi-Fi Antenna System Provides Superior Signal Quality, Coverage, and Technical Support.....	33
C. The Central Wi-Fi Antenna System Is Likely to Be Less Expensive than Continental's Individual Antenna	36
D. Passengers and Continental Employees Would Experience No Delay in Receiving High-Speed Internet Access	38
V. THE RESTRICTIONS ON CONTINENTAL'S ANTENNA ARE NECESSARY TO ACHIEVE LEGITIMATE SAFETY OBJECTIVES	39
A. The Safety Objectives Are Clearly Defined in the Lease Agreement and Other Readily Available Documents	40
B. The Antenna Restrictions Are Necessary to Achieve the Safety and Security Objectives	42
1. The Central Wi-Fi Antenna System Can Provide Security and Reliability to Certain Public Safety Operations.....	43
2. Interference Would Adversely Impact Current and Proposed Safety and Security Applications.....	48
C. Massport Narrowly Tailored Its Restrictions	52
D. The Restrictions Apply in a Nondiscriminatory Manner.....	54
VI. THE OTARD RULE SHOULD NOT APPLY TO CONTINENTAL'S WI-FI ANTENNA	55

TABLE OF CONTENTS

(continued)

	Page
A. Continental Is Not Covered by the OTARD Rule as a Reseller of Wireless Internet Access Service	55
B. The OTARD Rule Applies Only to Fixed Wireless Devices Used to Receive "Commercial" Non-Broadcast Communications Signals	59
C. The OTARD Rule Applies Only to Signals Originating or Terminating Outside of a Lessee's Exclusive-Use Premises	61
D. The FCC Has Never Enforced the OTARD Rule Against a Governmental Entity or Facility	64
E. The FCC Should Grant Airports the Same Exemption from OTARD that It Has Granted to Other Special-Use Facilities	64
F. Presidents Club Members Have No Rights Under the OTARD Rule	65
VII. THE FCC EXCEEDED ITS STATUTORY AUTHORITY IN APPLYING THE OTARD RULE TO WI-FI ANTENNAS	67
A. Congress Expressly Limited the FCC's Authority	67
B. The FCC May Not Rely on Its Ancillary Jurisdiction to Regulate the Installation of Wi-Fi Antennas	69
VIII. THE LEASE AGREEMENT DOES NOT AUTHORIZE CONTINENTAL TO INSTALL AND USE A WI-FI ANTENNA	72

EXECUTIVE SUMMARY

The Massachusetts Port Authority ("Massport"), an independent public authority of the Commonwealth of Massachusetts and the operator of Boston-Logan International Airport ("Logan"), submits these comments in support of its position that the Over-the-Air Reception Device ("OTARD") rule does not authorize Continental Airlines of Houston, Texas ("Continental") to continue using a Wi-Fi antenna in its private, members-only Presidents Club at Logan.

In a Petition for Declaratory Ruling, Continental asked the FCC for after-the-fact approval to install a 2.4 GHz Wi-Fi antenna for use by a handful of passengers who had purchased memberships to the Presidents Club. Continental subsequently amended its Petition to add that it now permits select employees to use the antenna. Although Continental and Massport had executed a Lease Agreement restricting Continental's use of the premises, which includes the Presidents Club, to specifically enumerated activities and prohibiting the placement of anything on the premises that may interfere with communications systems at Logan, Continental installed a Wi-Fi antenna in the Presidents Club, began offering wireless Internet access service, and interfered with the central Wi-Fi antenna system at Logan. Continental attempts to justify this breach of the Lease Agreement by claiming that its installation of a Wi-Fi antenna is consistent with the protections of the OTARD rule.

The FCC should reject Continental's request to continue to operate a Wi-Fi antenna to provide Internet access service for several compelling reasons: (1) Massport's installation of a central Wi-Fi antenna system, and its concomitant restriction on the installation of individual Wi-Fi antennas does not constitute an impairment under the OTARD rule; (2) Massport has

legitimate safety reasons for not allowing Continental to operate an individual Wi-Fi antenna; and (3) the OTARD rule does not apply to Continental's antenna.

As an airport operator in the post-9/11 world, Massport's primary function is to maintain a safe and secure facility for passengers and tenants in a highly complex environment. While Massport devotes a substantial amount of resources to ensure compliance with federal security regulations and to implement security programs, it also manages Logan to enable its tenants to conduct a myriad of aviation-related businesses and to provide the traveling public with world-class customer service. The difficulty of striking the appropriate balance between security and commercial/operational interests is compounded by the fact that Logan is one of the country's busiest airports and one of its most land-constrained airports. To accommodate the needs of security personnel, passengers, and tenants in a fair and reasonable manner, Massport exercises significant control over the terminal facilities at Logan through its leasing agreements and requires all tenants, including Continental, to use their leased premises only for certain enumerated purposes.

Massport has arranged for the installation of a neutral-host/common-use central Wi-Fi antenna system to ensure that all security personnel, tenants, and passengers have access to broadband communications at Logan. The central Wi-Fi antenna system offers numerous benefits for users, including optimal throughput, ubiquitous coverage throughout the terminals and on contiguous aircraft ramp areas, a high level of reliability, secure virtual private networks with encryption for confidential communications, and priority access for security personnel during emergencies. The Transportation Security Administration ("TSA"), the Massachusetts State Police, and three airlines already use, are scheduled to start using, or are considering the use of this central Wi-Fi antenna system for security-related communications. Many other

tenants and passengers also use the system for a variety of business and personal communications. The security and commercial operations on the central Wi-Fi antenna system will only increase over time.

The operation of the central Wi-Fi antenna system that everyone can use will prevent interference from congesting the unlicensed 2.4 GHz band at Logan. Continental's Wi-Fi antenna has caused interference with other users at Logan. This interference problem will only grow with the increased use of Wi-Fi devices, throughput limitations of the 2.4 GHz band, an increasingly densely populated airport environment, and existence of multiple, concurrent Wi-Fi systems in close proximity. Massport believes that the unique nature of Logan's environment requires a single, common-use infrastructure with radiofrequency management and load balancing to provide maximum spectrum utilization, optimal control over traffic priority, and the best-available method of maximizing throughput. The central Wi-Fi antenna system provides such an infrastructure.

Although Continental asks the FCC to ignore the complex balancing of these competing interests and apply the OTARD rule for the benefit of its exclusive club, the OTARD rule actually permits the restrictions in the Lease Agreement. In particular, Massport may restrict the installation and use of an individual Wi-Fi antenna in Continental's Presidents Club because it provides access to a central Wi-Fi antenna system. The FCC has stated that "the installation of a central antenna, and a concomitant restriction on the installation individual antennas, will not constitute an impairment" if the central antenna meets certain conditions. Massport meets those conditions because Logan's neutral-host/common-use Wi-Fi system (1) allows Continental to access its desired service and service provider; (2) provides superior signal quality, coverage, and technical support; (3) is less expensive than Continental's individual antenna; and (4)

imposes no delay on the transmission and reception of service. Although Continental's Presidents Club members do not qualify for protection under the OTARD rule, they would also receive many of these same benefits from the central Wi-Fi antenna system.

The central Wi-Fi antenna system at Logan also meets the safety exception to the OTARD rule because the proliferation of individual Wi-Fi antennas at Logan could cause radio interference and disrupt the existing or planned communications of the TSA, State Police, and other airlines. The Lease Agreement, as well as related documents, clearly define Massport's safety objectives and give Massport authority to prohibit the operation of Continental's Wi-Fi antenna.

Furthermore, the OTARD rule would not authorize Continental to install a Wi-Fi antenna in the Presidents Club in any event. The OTARD rule only protects antennas installed to serve the tenant as an "end user customer" and not antennas installed by the tenant to resell service to others, such as Continental's resale of Internet access service in the Presidents Club. Even if Continental were to claim that it does not resell Internet access service, it would still not qualify for the OTARD protections because the provision of "free" service does not meet the definition of "fixed wireless signal," which is a "*commercial* non-broadcast communications signal."

The OTARD rule also does not apply to Continental's Wi-Fi system because (1) the system is not needed by Continental to communicate with a service provider located outside of the Presidents Club; (2) Massport is a governmental entity that has restricted the installation and use of antennas as part of its responsibility for managing a sensitive governmental facility; (3) Massport has a unique relationship with its tenants and should qualify for an exemption similar to that granted to college and university dormitories; and (4) Continental's passengers are not airport tenants or lessees and, thus, have no OTARD rights.

Continental also has no authority to install a Wi-Fi antenna because the FCC exceeded its statutory authority in extending the OTARD rule to fixed wireless signals. The statutory language and legislative history demonstrate that Congress limited the FCC's OTARD authority to the prohibition of restrictions on the reception of video programming. While the FCC had relied on its ancillary jurisdiction to extend the OTARD rule, it lacks the general jurisdiction under Title I of the Communications Act to regulate the installation of Wi-Fi antennas.

Finally, even as Continental seeks to renege on its Lease Agreement with Massport, it claims that the Lease Agreement authorizes it to install a Wi-Fi antenna at the Presidents Club. Although Continental references several provisions that purportedly create an independent right to install a Wi-Fi antenna, these provisions instead confirm that the Lease Agreement permits only specifically enumerated activities, which do not include the installation and use of a Wi-Fi antenna.

BEFORE THE
Federal Communications Commission
WASHINGTON, D.C. 20554

In the Matter of)	
)	
Continental Airlines of Houston, Texas)	ET Docket No. 05-247
)	
Petition for Declaratory Ruling Regarding)	
Whether Certain Restrictions on Antenna)	
Installation Are Permissible Under the)	
Commission's Over-the-Air Reception Devices)	
(OTARD) Rules)	
 To: The Office of Engineering and Technology		

COMMENTS OF THE MASSACHUSETTS PORT AUTHORITY

The Massachusetts Port Authority ("Massport"), through its undersigned counsel, respectfully submits these Comments in response to the *Public Notice* in the above-captioned matter,¹ pursuant to Section 1.415 of the Federal Communications Commission's ("FCC") rules.² This proceeding addresses the authority of Massport to enforce the terms of its Lease Agreement with Continental Airlines of Houston, Texas, ("Continental") in connection with Continental's provision of public communications service in its "Presidents Club" at Boston-Logan International Airport ("Logan").

¹ OET Seeks Comment on Petition from Continental Airlines for Declaratory Ruling Regarding Whether Certain Restrictions on Antenna Installation Are Permissible under the Commission's Over-the-Air Reception Devices (OTARD) Rules, ET Docket No. 05-247, *Public Notice*, 20 FCC Rcd 13322 (2005). The Office of Engineering and Technology subsequently extended the deadline for filing comments to September 28, 2005, and the deadline for filing reply comments to October 13, 2005. OET Seeks Comment on Petition from Continental Airlines for Declaratory Ruling Regarding Whether Certain Restrictions on Antenna Installation Are Permissible under the Commission's Over-the-Air Reception Devices (OTARD) Rules, ET Docket No. 05-247, *Order Extending Comment Period*, DA 05-2335 (2005).

² 47 C.F.R. § 1.415 (2004).

I. INTRODUCTION

Continental has requested FCC approval to continue to operate a 2.4 GHz Wi-Fi antenna for use by passengers who have paid for the privilege of accessing Continental's private Presidents Club at Logan, irrespective of its Lease Agreement and Massport's objection to that installation.³ Although Continental claims that its request is consistent with the protections of the OTARD rule, the FCC has carefully crafted this rule to allow for special circumstances which exist in a highly complex environment such as Logan.

The FCC should approach Continental's request cautiously because an airport is different from a shopping mall, housing development, apartment building, or office building – premises that are the logical focus of the OTARD rule. Following the tragic events of 9/11, our nation's resources must be intensely focused on creating a safe and secure environment for the millions of airline passengers who travel every day. Massport also has to prepare for emergency situations, including Logan-specific events and natural disasters in its region, where Logan is recognized as part of a local and nationwide system of resources for homeland security. As the recent Katrina disaster has shown, the local airport is a critical facility for bringing emergency assistance to a stricken area. Logan is such a hub for the New England area. For all these reasons, Massport has made safety and security its highest priority, striving to meet the critical communications and other needs of the Transportation Security Administration ("TSA") and Massachusetts State Police, as well as the day-to-day operational and commercial concerns of all its tenants and passengers. Massport tries to accommodate the interests of everyone at Logan in a fair and reasonable manner. To reconcile the safety and security needs of the TSA and State Police with

³ Supplement to Petition of Continental Airlines, Inc. for a Declaratory Ruling, ET Docket No. 05-247 (July 27, 2005) [hereinafter *Supplemental Petition*]; Petition of Continental Airlines, Inc. for a Declaratory Ruling, ET Docket No. 05-247 (July 8, 2005) [hereinafter *Petition*].

the operational and commercial concerns of tenants and passengers, Massport restricted the installation of individual antennas and arranged for the deployment of a neutral-host/common use wireless data system.

The neutral-host Wi-Fi system is a central, open, cost-effective network that benefits all security personnel, tenants, and passengers. The central Wi-Fi antenna system also provides an operating environment that can be managed at a high level of reliability and low potential for interference for years to come. The TSA is considering using, and the State Police are scheduled to start using, this system for certain types of critical public safety communications. In addition, airlines and other tenants use Logan's Wi-Fi system for a variety of secure communications, such as baggage reconciliation, credit-card transaction processing, and Internet access. Passengers and tenants also use Logan's Wi-Fi system for wireless Internet access. The current uses of the system are diverse, and the potential security and commercial operations on this system will continue to expand in the future.

Continental argues that Massport cannot restrict the installation of an antenna in Continental's Presidents Club. Although Continental had agreed to such a restriction in its Lease Agreement, and the use of Continental's antenna creates a risk of interference for public safety and other users of Logan's central Wi-Fi antenna system, Continental insists that the OTARD rule should allow the installation and use of its individual antenna. In other words, Continental argues that its right to provide wireless Internet access service to approximately thirty-two preferential passengers a day outweighs the interests of the thousands of users of Logan's central Wi-Fi antenna system.

Massport cannot look at this issue in isolation, but must view it in light of the TSA, State Police, its other tenants, and passengers in the terminal areas that must be accommodated on the

same basis as Continental. Massport works closely on a day-to-day basis with its airline tenants who are its partners in ensuring the safety and security of the traveling public. Nevertheless, there are times when it is reasonable to restrict tenant activities in order to ensure that every tenant – as well as the millions of passengers that pass through Logan every year – can do so under the best possible conditions. Installation of competing antennas by multiple tenants will create an radiofrequency ("RF") environment that Massport believes will be virtually unmanageable and will consequently degrade the performance of all applications.

Although Continental asks the FCC to ignore the complex balancing of these competing interests, Massport believes that the FCC should protect the rights of all interested parties as much as possible. In an environment such as Logan, it is in the public interest for the FCC to permit a reasonable alternative for Wi-Fi access by tenants, such as that adopted by Massport. Massport, not Continental, has the responsibility for ensuring that all tenants can have an acceptable operating environment. The central Wi-Fi antenna system provides such an operating environment.

II. BACKGROUND

A. The Massachusetts Port Authority

Massport is an independent public authority of the Commonwealth of Massachusetts, created by act of the legislature in 1956 to own and operate Logan, L.G. Hanscom Field, the Tobin Memorial Bridge, and certain facilities within the Port of Boston.

1. Management Responsibilities

Logan is perhaps the most challenging management responsibility for Massport. While Massport's primary function as an airport operator is to maintain a safe and secure facility for airport users, it also has several non-security-related responsibilities.

An important aspect of Massport's management responsibility is to ensure compliance with federal statutes and regulations governing airport security. Federal law assigns Massport, as the operator of Logan, certain specific responsibilities with regard to the safety and security of the traveling public.⁴ One of the primary areas of responsibility for airport operators, such as Massport, is to control access to those areas where airplanes land, taxi, and take off – the Air Operations Area ("AOA") – and to certain other security-sensitive locations at the airport that are not open to the general public.⁵ Massport also must provide law enforcement support for its Airport Security Program, as well as for the TSA's passenger screening checkpoint activities.⁶

Since the tragic events of September 11, 2001, Massport has implemented enhanced security strategies, policies, and programs that meet and often exceed those required by the federal government.⁷ Logan was the first U.S. airport to receive the TSA's approval for its in-line hold baggage screening program.⁸ In September 2004, Logan was the first recipient of *Airport Security Report's* Exceptional Performance in Airport Security Award. Massport also continues to play a leadership role in the development of transportation security solutions, investing heavily in anti-terrorist training with a first-in-the-nation Anti-Terrorism Unit

⁴ E.g., 49 U.S.C. § 44903 (1997 & Supp. 2005); 49 C.F.R. pts. 1540 and 1542 (2004).

⁵ E.g., 49 C.F.R. § 1542.103; *see also id.* § 1542.203 (security of AOA); *id.* § 1542.207 (access control system for secured areas); *id.* § 1542.205 (airport identification media for security identification display area (SIDA)); *id.* § 1542.209 (background checks for unescorted access to SIDA).

⁶ 49 U.S.C. § 44903(c)(1); 49 C.F.R. § 1542.215.

⁷ Massachusetts Port Authority, Comprehensive Annual Financial Report, Year Ended June 30, 2004, at 8, http://www.massport.com/about/pdf/c_fy04_cafr.pdf [hereinafter *Financial Report*].

⁸ *Id.* at 26.

composed of specially trained and equipped officers, as well as an on-site bomb and weapons of mass destruction response team.⁹

In addition to these safety and security responsibilities, Massport has many other management duties. For example, as the property manager of Logan, Massport must negotiate agreements with tenants and prospective tenants seeking to initiate service, expand or contract their activities, or terminate their services at the airport. Massport also must resolve disputes between tenants involving the permissible uses of their leased space and other issues. To satisfy the needs of passengers and the local community, Massport must constantly improve the range of available services. Passenger and community satisfaction involves planning for future development, such as the construction of additional parking lots and the availability of better concessions for food and other services at Logan. Massport is also responsible for ensuring environmental compliance and supervising construction at Logan.

2. Size and Scope of Airport Facilities

These management responsibilities are heightened by the number of passengers and tenants that use the airport facilities. Logan was the most active airport in New England, the eighteenth most active airport in the United States, and the thirty-fifth most active airport in the world, based on total passenger volume in calendar year 2003.¹⁰ Passenger traffic increased by 14.6% in calendar year 2004 – from 22.7 million passengers to 26 million passengers¹¹ – and is

⁹ *Id.*

¹⁰ *Id.* at 2.

¹¹ Massachusetts Port Authority, Official Statement of the Massachusetts Port Authority Relating to Its \$192,135,000 Revenue Bonds, Series 2005-A (Non-AMT), \$29,725,000 Revenue Bonds, Series 2005-B (AMT), Periodic Auction Reset Securities (PARSSM), \$231,890,000 Revenue Refunding Bonds, Series 2005-C (Non-AMT) 30, http://www.massport.com/about/pdf/c_2005os.pdf [hereinafter *2005 Bonds, Series A, B and C - Official Statement*].

on pace to increase again in calendar year 2005.¹² To serve these passengers, Logan has six terminals, A, B, C, D, E, and Amelia Earhart, each with its own ticketing, baggage claim, and ground transportation facilities. As of December 31, 2004, Logan was served by fifty-six airlines, including six U.S. major air carriers, five low-cost carriers, sixteen non-U.S. flag carriers, and twelve regional and commuter airlines, with Continental Airlines providing 4.4% of the total passenger traffic.¹³

Although Logan is one of the country's busiest airports, it accommodates these airlines and passengers on a relatively small amount of land. Modern-day Logan evolved from a tiny airfield known as Boston Airport, which was built by the U.S. Army in the early 1920s on 189 acres of tidal flats in East Boston. Over the years, the U.S. Army and subsequently the Commonwealth of Massachusetts expanded the size of the airport by filling portions of Boston Harbor. The airport boundary currently encompasses approximately 2,400 acres in East Boston, which is small in comparison to most airports with a significant passenger volume. By contrast, Denver International Airport covers approximately 34,000 acres,¹⁴ and Houston's George Bush Intercontinental Airport, which is in the city of Continental's corporate headquarters and is its primary hub, has more than 10,000 acres.¹⁵ Because Logan has five runways, fourteen miles of taxiway, and 237 acres of concrete and asphalt apron within its 2,400 acres, the space left for the actual terminals is quite small. These cramped quarters require Terminal E alone to house

¹² Boston-Logan International Airport, Monthly Airport Traffic Summary – July 2005, http://www.massport.com/logan/pdf/c_stats_jul05.pdf.

¹³ *2005 Bonds, Series A, B and C - Official Statement* 31, 32.

¹⁴ Denver International Airport, About DIA, <http://www.flydenver.com/guide/index.asp> (last visited Sept. 12, 2005).

¹⁵ Houston Airport System, George Bush Intercontinental Airport, <http://iah.houstonairportsystem.org/about> (last visited Sept. 12, 2005).

twenty-six airlines, including four airlines with hospitality clubrooms adjacent to each other, and numerous other tenants. The tightly confined airport premises makes management of RF facilities extremely challenging.

3. Leasing Arrangements

To satisfy these safety, security, and overall management responsibilities, Massport exercises significant control over terminal facilities at Logan through its leasing arrangements with airlines and other tenants. In 2003, Continental and Massport executed a Lease Agreement regarding the use of space in Terminal C at Logan.¹⁶ Continental agreed in the Lease Agreement to restrict its use of the Premises, specifically agreeing that "[t]he Premises shall be used only for the . . . [Permitted Uses] in accordance with the provisions specified herein, *and for no other purposes whatsoever*."¹⁷

In the Lease Agreement, Continental agreed to numerous restrictions to its Permitted Uses. One of these restrictions, described in the text of the Lease Agreement and confirmed in subsequent correspondence, requires that Continental:

shall not do or knowingly permit to be done anything which may interfere with the effectiveness or accessibility of any . . . communications system, key card access systems, . . . electrical system, fire-protection system, sprinkler system, alarm system, . . . installed or located on, under, in or adjacent to the Premises now or in the future.¹⁸

In addition, Continental agreed that it would not make any alterations, including the installation of communications equipment, without submitting an application and receiving the

¹⁶ Boston-Logan International Airport, Terminal Lease between The Massachusetts Port Authority and Continental Airlines, Inc., L-7936, attached as Exhibit A [hereinafter *Lease Agreement*].

¹⁷ *Id.* § 7.1 (emphasis added).

¹⁸ *Id.* § 10.3(iii); *Petition* at Exhibit A, Exhibit C.

prior approval of Massport.¹⁹ In particular, section 9.4 provides that "[t]he Tenant [Continental] shall not *place* or construct any improvements, structures, alterations, modifications, signs, *communications equipment, wiring* or additions in, to, or upon the Premises . . . without prior written approval"²⁰ Section 9.8 of the Lease Agreement requires Continental to "submit a complete Tenant Alteration Application ("TAA")" to propose the placement of communications equipment in the Presidents Club.²¹ The TAA clearly requires "preliminary engineering, architectural plans or other information" relevant to the proposal and a refundable deposit or bond.²² Once the tenant submits a TAA, Massport employees review the proposal to ensure that it adequately addresses the various safety/security concerns highlighted in the Lease Agreement.

Continental also agreed to use its leased space only for certain enumerated Permitted Uses²³ and "not [to] use the Premises for any use not specifically granted herein without the prior written approval of the Authority [Massport]."²⁴ The limitations of the Permitted Uses to air transportation are clear in sections 7.1(a)(iv) and 7.1(a)(xi), which refer to "operations, communications, reservations, and administrative office functions and activities in connection with *air transportation* performed by Tenant"²⁵ and "the installation, operation, and maintenance of telecommunications equipment customarily used in *air transportation* operations, subject to

¹⁹ *Lease Agreement* §§ 7.2(h), 9.4, 18.1, attached as Exhibit A; *Petition* at Exhibit A, Exhibit C.

²⁰ *Lease Agreement* § 9.4 (emphasis added), attached as Exhibit A.

²¹ *Id.* § 9.8.

²² *Id.*

²³ *Id.* § 7.1.

²⁴ *Id.* § 7.2.

²⁵ *Id.* § 7.1(a)(iv) (emphasis added).

approval under the TAA Process."²⁶ Besides the fact that all Permitted Uses are restricted by various provisions in the Lease Agreement, as discussed above, these Permitted Uses clearly do not contain any reference to non-air transportation activities, such as the installation of any wireless communications equipment in the Presidents Club or the installation and use of equipment for an information service, such as wireless Internet access service.

It is disingenuous to assert that the provision for quiet enjoyment in section 19.2 somehow negates the numerous provisions in the Lease Agreement that specify and restrict Continental's uses under the Lease Agreement.²⁷

While the Lease Agreement makes clear that Continental is not permitted to engage in certain activities and that Massport itself does not necessarily have any responsibility to provide any services, such as telecommunications or data communication services in the Presidents Club, to Continental,²⁸ there are suppliers, vendors, and contractors operating at Logan which Continental has agreed to use.²⁹ In the case at issue here, Continental may still receive wireless Internet access service through the central Wi-Fi antenna system.

Despite agreeing on numerous provisions and restrictions in the Lease Agreement, and without seeking any prior approval from Massport, Continental installed a Wi-Fi antenna in its Presidents Club for the use of preferential passengers who pay a membership fee. The transmissions from Continental's Wi-Fi antenna subsequently interfered with the effectiveness and accessibility of the central Wi-Fi antenna system at Logan.

²⁶ *Id.* § 7.1(a)(xi) (emphasis added).

²⁷ *Id.* § 19.2.

²⁸ *Id.* § 10.1(d).

²⁹ *Id.* § 8.5.

B. Description of Central Wi-Fi Antenna System

Logan has a Wi-Fi system that delivers services and is optimal from an RF standpoint to make it secure and effective for all users. The term "Wi-Fi" "refer[s] to any product or service using the 802.11 series standards developed by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area network connections."³⁰ "Wi-Fi enabled wireless devices, such as laptop computers or personal digital assistants (PDAs), can send and receive data from any location within signal reach of a Wi-Fi equipped base station or access point (AP)."³¹

The Wi-Fi system at Logan was installed by Advanced Wireless Group, LLC ("AWG"). Massport selected AWG to design and build the Wi-Fi system through a public bidding process. The public bidding process revealed that AWG has substantial experience with Wi-Fi systems and similar implementations worldwide. In particular, the AWG team has extensive experience in narrowband and broadcast wireless and technology deployments in over 2,700 venues around the world and has specified or installed over 30,000 Wi-Fi access points in airports, universities, hospitals, stadiums, and other public facilities. The AWG team has also worked with numerous Wi-Fi implementations within managed venues similar to Logan.

AWG designed the Wi-Fi system for Terminals A, B, C, D, and Amelia Earhart to integrate it with the existing Massport Universal Wireless Ethernet system in Terminal E. The system supports wireless data transmission/reception using IEEE 802.11b/g, which operate on an unlicensed basis in the 2.4 GHz band and are compatible with other standards and emerging

³⁰ Availability of Advanced Telecommunications Capability in the United States, GN Docket No. 04-54, *Fourth Report to Congress*, 19 FCC Rcd 20540, 20557 (2004) [hereinafter *Fourth Report to Congress*].

³¹ *Id.*

technologies.³² AWG designed the system to maximize throughput and service quality by employing three non-overlapping, independent channels rather than all eleven channels in the 2.4 GHz band. Although the IEEE 802.11g standard has an advertised throughput of 54 Mbps per channel, AWG has observed that the maximum sustained transfer rate from an access point is approximately 22 Mbps with no associated 802.11b devices and approximately 14 Mbps with associated 802.11b devices.

AWG has installed approximately 245 access points throughout the terminals to provide contiguous coverage, overlap, and hand-off (roaming) from the curb of the terminal to the tail of the airplane. To ensure that each user receives optimal throughput, Logan's central Wi-Fi antenna system associates users to access points based on the signal strength, available bandwidth, client adapter settings, and/or number of users on a particular access point at any given time. A third-party consultant recently confirmed the ubiquitous coverage of the central Wi-Fi antenna system, measuring strong (> -70 dBm) signal strength throughout most of the tested terminal areas.³³

Logan's central Wi-Fi antenna system also has several redundancies and safeguards. For example, the system features overlapping coverage, redundant wired backbone to the distribution switch layer, redundant access control, routers and firewalls, Power-Over-Ethernet with Battery Backed up Uninterruptible Power Supply to protect from power outages to ensure high availability and quality of service for all users. The system also has multiple wireline

³² Wireless Broadband Access Task Force, Federal Communications Commission, *Connected & On the Go: Broadband Goes Wireless*, GN Docket No. 04-163, *Report*, 19-20 (Feb. 2005) [hereinafter *Task Force Report*]. Access points in some terminals are also enabled for 802.11a, which operates in the unlicensed 5 GHz band.

³³ Beyond Wire, *Wireless Engineering Audit: Enterprise Wireless Network* 21, 23, 25, 27 (Sept. 16, 2005), attached as Exhibit B [hereinafter *Engineering Audit*].

connections to two wireless Internet service providers. Thus, the system is a robust, redundant, and standardized high-speed wireless LAN that spans the entire terminal area of the airport.

This central Wi-Fi antenna system accommodates numerous private users at Logan by supporting secure virtual private networks with encryption for their confidential communications.³⁴ AWG has allocated multiple "virtual local area networks" ("VLANs") to private users, currently up to 15 per access point in addition to the public VLAN, and has provided a minimum of one DMZ switch in each terminal for private user entry.³⁵ While the central Wi-Fi antenna system also supports most authentication and encryption standards and protocols via Cisco Secure ACS, or hands-off virtual local area network authentication/encryption to the user's systems, AWG has indicated that it will support any new, technologically feasible standards and protocols as well. Thus, these private users may implement their own VPNs with pre-established log-on scripts to allow for private tunneling into the system using VPN and IPSec.

The central Wi-Fi antenna system also affords priority treatment for certain types of users. AWG designed the central Wi-Fi antenna system to have the capability of providing priority access across the whole network for their operations. The prioritization levels for Logan are (1) safety/security (TSA and Massachusetts State Police), (2) Massport, (3) airlines, and (4) the public. This priority access would enable AWG to dedicate the entire central Wi-Fi antenna system for public safety communications in the event of another 9/11 type emergency, while also having the ability to terminate all network use by the public and/or other selected private users, if

³⁴ The FCC's Wireless Broadband Access Task Force recognized that "technological advances are enabling more secure wireless networks, safeguarding the confidentiality of information transmitted over the network." *Task Force Report* at 40.

³⁵ A DMZ switch is a part of a network that is protected by a firewall but may be accessed by external Internet clients.

required by the TSA or State Police, within minutes, which would not be possible if tenants had their own individual Wi-Fi antennas. This ability is similar to the cellular communications blackout that was instituted in the New York City subway tunnels immediately following the terrorist event in London in July 2005.

The TSA, Massachusetts State Police, and three airlines use, are scheduled to start using, or are considering the use of the central Wi-Fi antenna system for communications related to the safety and security of the airport environment. In July 2005, the TSA instituted a pilot program to determine if the central Wi-Fi antenna system "would be suitable for transmitting communications between its security checkpoints and its central administrative office."³⁶ Although the TSA did not transmit any security-related information during the pilot program, the results were so promising that the TSA plans "to explore other possible uses of this communications system."³⁷ Thus, the TSA has tested and is considering the use of the central Wi-Fi antenna system to transmit security-related communications necessary to protect the nation's transportation system.

The State Police is scheduled to start using Logan's central Wi-Fi antenna system in the near future. As the FCC's Wireless Broadband Access Task Force³⁸ anticipated, a central Wi-Fi

³⁶ Letter from Dennis J. Cronin, Regional Counsel, Transportation Security Administration, to Deborah Lau Kee, Associate Deputy Chief Legal Counsel, Massachusetts Port Authority (Sept. 27, 2005), attached as Exhibit C.

³⁷ *Id.*

³⁸ The Wireless Broadband Access Task Force was established in May 2004. FCC Task Force Recommends Actions to Speed the Rollout of Wireless Broadband Services to Consumers Across America, News Release (Feb. 10, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-256694A1.pdf. "Comprised of a team of multidisciplinary staff from across several FCC Bureaus and Offices, the Task Force examined technological developments in wireless broadband, surveyed existing and anticipated applications, and conducted a comprehensive review of the Commission's wireless broadband policies." *Id.*

antenna system "significantly enhances the information available to [State Troopers] . . . on patrol via their mobile data computers."³⁹ The State Police has purchased 144 hand-held wireless computers, Hewlett Packard iPAQ devices, and are scheduled to deploy them on an additional secure connection through the central Wi-Fi antenna system. State Troopers must use the iPAQ device as part of their critical public safety communications because it is the only wireless handheld technology presently certified for use by the Massachusetts Criminal Justice Information System ("CJIS"), which is the state agency through which the State Police may access law enforcement information from the FBI's National Crime Information Center and from data repositories in other states via the National Law Enforcement Telecommunications System. Because the central Wi-Fi antenna system can support iPAQ it will allow the State Police to communicate on a secure network, which is not always achievable with private radio spectrum that is sometimes susceptible to monitoring by radio scanners.⁴⁰

Massport understands that the State Police plans to deploy a new PocketCop™ software application on the central Wi-Fi antenna system that will provide mobile access to images and data. This application will enable State Troopers on foot patrol to conduct identification and background checks on passengers and suspects. State Troopers will have access to a variety of information, including driver license information, vehicle registrations, stolen vehicle information, weapon registrations, and wants and warrant information. Speed and accuracy of suspect information is a fundamental weapon for first responders. The PocketCop™ application

³⁹ *Task Force Report* at 38.

⁴⁰ E.g., Jim Rendon, *Notebooks and Wi-Fi Keep Colorado Cops on the Beat*, SearchMobile Computing, Mar. 8, 2004, http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci953936,00.html.

will allow State Troopers at Logan to access critical information quickly, which will permit them to do their jobs more efficiently, more effectively, and, most importantly, more safely.

The State Police is also considering using the central Wi-Fi antenna system to interface with a guided mobile device ("remote-controlled robot"). The greater range of the central Wi-Fi antenna system will allow images to be sent from the remote-controlled robot back to the central communications center, as well as to the local control unit. The ability to use the central Wi-Fi antenna system will eliminate the need for the local control unit to accompany the remote-controlled robot and will allow greater flexibility in the use of the remote-controlled robot in internal as well as external environments.

The central Wi-Fi antenna system will also be important to the State Police because of the ability to send images, the ability to accommodate mobile personnel, the ability to prioritize safety and security transmissions, the geographic coverage both inside the passenger terminal and outside on the aircraft ramp, and the redundancy available as a component of the overall airport communications system.

Future safety and security applications at Logan could include (1) real-time, full-motion video from any location to any other location; (2) live video from an emergency scene to a command center; (3) accessing mug shots from the field; (4) mapping/location-based services; (5) digital image transfers; (6) large file transfers; and (7) bio-terrorism detection and response information.

Three airlines also rely on the central Wi-Fi antenna system for safety and security communications. In particular, British Airways, Virgin Atlantic, and United use the central Wi-Fi antenna system for baggage reconciliation. Baggage reconciliation is a security procedure which requires that baggage loaded on an aircraft be matched with the passengers who board that

aircraft. This anti-terror measure was implemented to address the risks of unassociated baggage being used as a terrorist weapon.

The central Wi-Fi antenna system permits airlines to track the location of baggage both within the terminal and on the aircraft ramp area using handheld devices on a private VLAN. Employees may scan bags and upload information real-time over the central Wi-Fi antenna system without having to make repeated trips to their desks. The coverage of the central Wi-Fi antenna system enables airlines to track baggage from the cargo hold of the aircraft, to an adjacent terminal, and into the cargo hold of another aircraft for the connecting flight. Because AWG has deployed access points throughout the passenger terminals *and* the aircraft ramp area at Logan, airlines have seamless access to the network and control over the bags even as they move between leased areas within terminals and onto non-leased areas such as the aircraft ramp area.

In addition to these safety-related applications, Massport and several other tenants use the central Wi-Fi antenna system for private, internal communications. For example, Massport employees operate handheld Flight Information Display System ("FIDS") devices that provide a state-of-the-art information display system with real-time updates of flight information. The central Wi-Fi antenna system is or has been used by twelve concessionaires for credit-card transaction processing, one airline for ticketing and temporary data facilities, and three contractors for Internet access. Other potential applications include mobile service curbside check-in, roving ticket agents, fleet management, fuel management, catering management, and freight company access for terminal pick-up and traffic scheduling.⁴¹

⁴¹ The Airports-Council International-North America has stated that possible uses of unlicensed wireless systems may include baggage handling, gate operation functions, portable check-in
(continued...)

The central Wi-Fi antenna system also provides an intuitive user interface and is configured for simplified public user access. The system averages 40,000 visits to the web site and 10,000 paid users per month, which is significantly more than the estimated 32 preferential passengers that use the Continental system per day.⁴² The user merely needs to turn on a laptop computer or PDA, insert a Local Area Network ("LAN") card, if necessary, and launch a web browser to connect automatically to the Wi-Fi web site for Logan. From the main screen, the user may access free information from www.loganwifi.com or www.massport.com, such as news, weather, flight and gate information, and local restaurants.⁴³

The user may also connect to the Internet or to a corporate network. If the user elects to connect to the Internet, the central Wi-Fi antenna system offers a neutral host/common use wireless data network. This network design enables a single, integrated wireless broadband system to accommodate public domain access for subscribers using different wireless providers. Public domain access is supported via (1) a credit card transaction; (2) the use of a prepaid or promotional usage card from an airport vendor or vending machine; (3) the normal log-on

facilities, and desk-to-passenger communications on airline schedule changes. *Task Force Report* at 37 (citing Comments of Airports-Council International-North America, GN Docket No. 04-163 (June 3, 2004)).

⁴² *Petition* at Affidavit in Support of Petition of Continental Airlines, Inc.

⁴³ <http://www.loganwifi.com/splash/default2.sps>. LoganWi-Fi.com has generated several positive comments from travelers. For example, one traveler praised the system for providing "timetable, arrival, and departure info," as well as "access to radar information up to 90 miles out – all for free." Peter Cochrane's Blog: Information the Way It Should Be, <http://networks.silicon.com/mobile/0,39024665,39152192,00.htm> (Sept. 12, 2005). This traveler also reported that "entertainment listings, eating houses, hotels, transport, weather, CNN news, sport and other events are all available too. Cool or what?" *Id.*

scripting from a pre-arranged account with an authorized wireless Internet service provider or one of its partners; (4) an agreement between a tenant and AWG.⁴⁴

The first two alternatives permit access at a nominal rate of up to \$7.95 for twenty-four hour access.⁴⁵ The third alternative enables an airport visitor to use the central Wi-Fi antenna system without paying any additional fee to AWG or Massport. In a little over one year since start-up, AWG has authorized two service providers, iPass and Boingo, on its central Wi-Fi antenna system and has entered into negotiations with three other major providers. iPass has more than 600 Internet service provider or reseller partners.⁴⁶ Boingo is a Wi-Fi "hot spot" aggregator that allows other Internet service providers to extend their reach and has, or will soon have, agreements with several major service providers, including Earthlink, Fiberlink, BT Infonet, MCI, Nextel, and Skype.⁴⁷ If a user has a direct agreement with iPass or Boingo, or with one of their partners, the user may gain secure Internet access at no extra charge from AWG or Massport. The user merely needs to select its preferred Internet service provider from the drop-down list on Logan's Wi-Fi page, enter a user name and password, and access the Internet.

Finally, under the fourth alternative, users may access the central Wi-Fi antenna system as customers of tenants that have an agreement with AWG. If a tenant has no relationship with iPass, Boingo, or one of their Internet service provider or reseller partners, the tenant may enter

⁴⁴ AWG and Massport receive a portion of the revenues from wireless Internet access service, regardless of whether the customer accesses the central Wi-Fi antenna system by credit card, prepaid card, through a direct agreement with a wireless Internet service provider or Internet service provider, or through a tenant's agreement with AWG.

⁴⁵ Cards are also made available through promotional offers from sponsors of the central Wi-Fi antenna system and other vendors.

⁴⁶ *Minneapolis Airport Gets Neutral-Host Wi-Fi*, m-Travel.com, Apr. 8, 2002, http://www.m-travel.com/news/2002/04/minneapolis_air.html.

⁴⁷ Boingo Wireless, <http://www.boingo.com>.

into an agreement with AWG that will allow the tenant's customers to receive wireless Internet access service on its premises.

C. Interference

Interference has become a major concern for the Wi-Fi system at Logan. As noted in the February 2005 report of the FCC's Wireless Broadband Access Task Force ("Task Force"), "as more and more devices use a particular unlicensed band in a localized area, interference mitigation will become increasingly important and, correspondingly, more technically complex."⁴⁸ The public interest requires Massport to manage critical spectrum resources in this special-use governmental facility to ensure that everyone may use unlicensed wireless devices with minimal potential for interference, and to allow the police and security forces working at Logan to integrate their devices into an effective emergency and security system with minimal disruption to every-day applications.

At Logan, this interference results from the increased use of 2.4 GHz devices, the densely populated airport environment, the relatively tight confines of Logan, and the existence of multiple, concurrent Wi-Fi systems in close proximity. Even the *Task Force Report* supported the use of private efforts to reduce interference,⁴⁹ and Massport believes that the unique nature of the Logan environment requires a single, common-use infrastructure with RF management and load balancing to provide maximum spectrum utilization, optimal control over traffic priority, and the best-available method of maximizing throughput.

The use of 802.11b/g wireless local area network technology has increased in recent years. In 2004, the FCC noted that "[t]he expansion of Wi-Fi access to the Internet has recently

⁴⁸ *Task Force Report* at 57.

⁴⁹ *Id.* at 57-59.

seen the explosive growth of hotspots on a commercial and noncommercial basis." In 2005, the FCC's Task Force agreed that "the number of wireless 'hot spots' using Wi-Fi technologies [has] . . . grown exponentially and may number as many as 150,000 by the end of 2005."⁵⁰ The Task Force also cited industry analysts as projecting "that the number of hot spot users worldwide will total 30 million by the end of 2004, up from 9.3 million in 2003 and 2.5 million in 2002."⁵¹ Massport has documented an increase in the number of unauthorized Wi-Fi access points at Logan over the past two years, despite its efforts to prevent the proliferation of these actual and potential sources of interference.⁵² While this popularity has resulted in an increased number of Wi-Fi devices and users, it has also influenced the shift of wireless applications from text- and html-based applications to bandwidth-intensive applications, such as voice and streaming video.

This explosive growth of users and bandwidth-intensive applications has strained the limited throughput resources for data transmissions in the 2.4 GHz band. The 2.4 GHz band supports only three non-overlapping, independent channels in a properly deployed Wi-Fi system. Although the advertised throughput of each of the 802.11g channels is 54 mbps, AWG has observed that the maximum sustained transfer rate is actually 22 mbps with no associated 802.11b devices and 14 mbps with associated 802.11b devices. Based on these practical limitations, the total, maximum data throughput for the 2.4 GHz band is 66 mbps with no associated 802.11b devices and 42 mbps with associated 802.11b devices.

The airport environment presents a unique density problem because Logan hosts so many tenants and passengers in such a small area. As described above, Logan is one of the most active

⁵⁰ *Id.* at 3.

⁵¹ *Id.* at 30; see *Fourth Report to Congress*, 19 FCC Rcd at 20557-58 (citing industry analysts as "predict[ing] the continued growth of Wi-Fi access points . . .").

⁵² *Engineering Audit* at 35-36, attached as Exhibit B.

airports in the country based on passenger volume, and it houses numerous airlines, restaurants, and concessionaires over a relatively small geographic area. If tenants could install and use individual Wi-Fi systems, the aggregate signals would easily exceed the available spectrum capacity in the confined space of the airport terminal and prevent efficient and effective use for everyone. The existence of multiple, concurrent Wi-Fi systems in close proximity, each with a potentially different design and channel set up, would create unpredictability and interference for users as they move in and out of range of different tenant's Wi-Fi systems located around the terminal. Current PDAs are particularly susceptible to interference because the existing technology cannot isolate a specific Wi-Fi network for operation and is captured by the strongest signal in the vicinity. Because of this characteristic, the users of PDAs could have their data transmissions interrupted or delayed by a stronger signal emanating from a nearby access point. In other words, as a PDA user passes by an access point with a stronger signal, the PDA could attempt to connect to the stronger signal of that access point, could drop its original signal, and could have its data transmissions interrupted and/or lost. Because of these interruptions and delays, the PDA could constantly have to re-authenticate, search for a less congested channel, and retransmit signals.

Logan already experiences this type of interference. A third-party consultant has documented actual interfering and competing signals from unauthorized access points operating in the terminals across all channels, including degradation to the central Wi-Fi antenna system from Continental's individual Wi-Fi antenna near the TSA checkpoint in Terminal C.⁵³ This interference problem is exacerbated because Wi-Fi operators, such as Continental, do not confine their Wi-Fi signals to their premises. For example, an AWG employee was present as a laptop

⁵³ *Id.* at 15, 30.

user in the gate area of another airline opened his computer and, instead of receiving the central Wi-Fi antenna system, connected to Continental's Wi-Fi system transmitting from the Presidents Club. This employee also witnessed another user accessing the Continental's Presidents Club Wi-Fi antenna while in a nearby restaurant. A Massport employee connected to Continental's public Wi-Fi system in front of, and in a public eating area bordering, the Presidents Club. AWG even discovered at one point that Continental's signal extended to another terminal altogether.

Massport must look at the interference issues beyond the specifics of Continental's antenna because, by extension, every tenant and storefront at Logan could want to install a similar Wi-Fi antenna. Massport believes that common methods of interference mitigation would not adequately resolve the interference problem. As explained below, channel mapping, reducing the power of competing Wi-Fi systems, and the use of alternative spectrum would not provide the same advantages as RF management through a central Wi-Fi antenna system.

Channel Mapping. Channel mapping and least congested channel techniques would not resolve interference in the long term. The term "channel mapping" refers to dedicating each of the three discrete 2.4 GHz channels to a particular type of user, such as safety and security personnel, tenants, and public users. If a large number of tenants sought to use the single channel, however, it could reduce channel availability on the central Wi-Fi antenna system, preclude higher bandwidth applications, and limit the number of applications that can run simultaneously. The number of potential access points/networks could exceed the ability of software to change channels, which would mean that access points would never stop migrating. Conversely, if only a limited number of tenants used the designated channel, such as Continental's claim of a mere 32 users in the Presidents Club per day, the channel would go to

waste, while other users might not have enough bandwidth. In addition, the dedication of channels to specific users would require a separate set of access points for each type of user. Finally, channel mapping would not work because PDAs are not currently capable of channel programming.

Power Reduction. Individual Wi-Fi antenna users could also not simply "power down" their systems. Although a reduction in power might mitigate somewhat Continental's interference with other Wi-Fi systems on the same floor, its system could still interfere with antennas on floors above and below it, including locations where the baggage reconciliation process takes place. In addition, tenants would not necessarily know the identity of other Wi-Fi operators, the location of the competing antennas, the coverage area of those systems, or when to power down without some type of over-arching RF management structure.

Alternative Spectrum. Public safety agencies can enhance their available communications tools through the use of the central Wi-Fi antenna system at Logan. While public safety agencies still use their licensed frequencies for mission-critical operations (such as voice transmissions), the central Wi-Fi antenna system provides them with cost savings, enhanced functionalities (such as image, data, and video transmissions), a secure network, and redundancy and reliability that are not available through the use of their licensed spectrum at the Airport. Wi-Fi also provides public safety agencies with the flexibility to operate throughout the airport and to choose from a wide variety of commercially available equipment.

The central Wi-Fi antenna system at Logan would resolve these interference problems by providing a single, common-use infrastructure with RF management and load balancing. This system provides maximum spectrum utilization for all users by providing three discrete channels for operations. The RF management and load balancing offers optimal control over traffic

priority, known as Quality of Service ("QOS"), allocating bandwidth to different classes of users based on the nature of the operations, *e.g.*, safety/security, police, Massport, airlines, and the general public. The QOS essentially predetermines the amount of throughput for certain classes of users and adjusts that amount based on those criteria as conditions change. The QOS enables the central Wi-Fi system to accommodate an increase in the number of users, without compromising vital safety and security communications. Finally, a central Wi-Fi system provides the best-available means of mitigating the interference problem because it eliminates the incompatible technological designs and channel set-ups associated with the deployment of multiple, unmanaged, concurrent Wi-Fi systems.

III. APPLICABLE LAW AND STANDARD OF REVIEW

Section 207 of the Telecommunications Act of 1996 requires the FCC to "promulgate regulations to prohibit restrictions that impair a viewer's ability to receive video programming services through devices designed for over-the-air reception of television broadcast signals, multichannel multipoint distribution service, or direct broadcast satellite services."⁵⁴

On August 6, 1996, the FCC issued a *Report and Order, Memorandum Opinion and Order, and Further Notice of Proposed Rulemaking* adopting section 1.4000 of its rules to implement section 207.⁵⁵ Section 1.4000 prohibits governmental and private restrictions that impair the ability of antenna users to install, maintain, or use over-the-air reception devices

⁵⁴ Telecommunications Act of 1996, Pub. L. 104-104 § 207, 110 Stat. 56, 114 (1996).

⁵⁵ *In re Preemption of Local Zoning Regulation of Satellite Earth Stations; In re Implementation of Section 207 of the Telecommunications Act of 1996 Restrictions on Over-the-Air Reception Devices*, IB Docket No. 95-59, CS Docket No. 96-83, *Report and Order, Memorandum Opinion and Order, and Further Notice of Proposed Rulemaking*, 11 FCC Rcd 19276 (1996) [hereinafter *OTARD Report and Order*].

("OTARD").⁵⁶ The FCC subsequently relied on its ancillary jurisdiction to extend the OTARD rule beyond the plain language of section 207 to encompass not only devices that receive video programming, but also devices that transmit and receive fixed wireless signals.⁵⁷

The OTARD rule applies to restrictions on antennas "one meter or less in diameter or diagonal measurement" that are "on property within the exclusive use or control of the antenna user where the user has a direct or indirect ownership or leasehold interest in the property"⁵⁸ The rule prohibits any restriction that "impairs the installation, maintenance, or use of an antenna if it: (1) [u]nreasonably delays or prevents installation, maintenance, or use; (2) [u]nreasonably increases the cost of installation, maintenance, or use; or (3) [p]recludes reception or transmission of an acceptable quality signal."⁵⁹ The FCC has interpreted this impairment standard to allow property managers to require the use of a central antenna, and to restrict the use of individual antennas, if the central antenna meets certain conditions.⁶⁰ The FCC also adopted a

⁵⁶ 47 C.F.R. § 1.4000.

⁵⁷ In re Promotion of Competitive Networks in Local Telecommunications Markets, WT Docket No. 99-217, *First Report and Order and Further Notice of Proposed Rulemaking*, 15 FCC Rcd 22983, 23027-23038 ¶ 97-124 (2000) [hereinafter *Competitive Networks First Report and Order*]. In 2004, the Office of Engineering and Technology issued a *Public Notice* stating that the OTARD rule also applies "to the operation of unlicensed equipment, such as Wi-Fi access points" Commission Staff Clarifies FCC's Role Regarding Radio Interference Matters and It Rules Governing Customer Antennas and Other Unlicensed Equipment, *Public Notice*, 19 FCC Rcd 11300, 11300 (2004) [hereinafter *Unlicensed Devices Public Notice*]. If the *Public Notice* represented a interpretation of the OTARD rule, it lacks "the force and effect of law and would not be accorded that weight in the adjudicatory process." *Shalala v. Guernsey Memorial Hospital*, 514 U.S. 87, 99 (1995). Conversely, if the *Public Notice* "adopted a new position inconsistent with any of the [FCC's] existing regulations," *id.* at 100, it violated the notice-and-comment rulemaking requirement. 5 U.S.C. § 553(b) (1996).

⁵⁸ 47 C.F.R. § 1.4000(a)(1).

⁵⁹ *Id.* § 1.4000(a)(1), (3).

⁶⁰ In re Implementation of Section 207 of the Telecommunications Act of 1996; Restrictions on Over-the-Air Reception Devices, CS Docket No. 96-83, *Order on Reconsideration*, 13 FCC Rcd 18962, 18999 ¶ 88 (1998) [hereinafter *OTARD Order on Reconsideration*].

safety exception that permits prior approval requirements and other restrictions that are necessary to accomplish a legitimate safety objective, as long as the restrictions are narrowly tailored, impose as little burden as possible, and apply in a nondiscriminatory manner throughout the regulated area.⁶¹

To the extent the rule applies, Massport bears the burden of demonstrating compliance with the OTARD rule.⁶² Although Continental neglected to provide many facts about its Wi-Fi system that would enable Massport to irrefutably demonstrate compliance under the OTARD rule, Massport believes that the following sections demonstrate its compliance with the central antenna approach and safety exception. Moreover, based on the facts averred in Continental's *Petition* and *Supplemental Petition*, Massport also questions the applicability of the OTARD rule to this situation.

IV. THE EXISTENCE OF A CENTRAL ANTENNA SYSTEM PERMITS MASSPORT TO RESTRICT THE INSTALLATION AND USE OF CONTINENTAL'S ANTENNA

The FCC permits property managers to restrict the installation and use of an individual antenna otherwise protected under the OTARD rule, as long as they offer access to a central antenna. Because Logan has a central Wi-Fi antenna system, Massport may restrict the installation and use of an individual Wi-Fi antenna in Continental's Presidents Club under the Lease Agreement.⁶³

⁶¹ 47 C.F.R. § 1.4000(b)(1); *see In re Frankfurt*, CSR-5238-0, *Memorandum Opinion and Order*, 16 FCC Rcd 2875, 2886 ¶ 31 (2001); *OTARD Order on Reconsideration*, 13 FCC Rcd at 18981 ¶ 41.

⁶² 47 C.F.R. § 1.4000(g).

⁶³ *Petition* at Exhibit C.

Section 1.4000 of the FCC's rules prohibits any law, regulation, or restriction that "impairs installation, maintenance, or use of an antenna."⁶⁴ In an *Order on Reconsideration*, the FCC ruled that "the installation of a central antenna, and a concomitant restriction on the installation of individual antennas, will not constitute an impairment . . . if, like any other restriction, it does not impair installation, maintenance, and use."⁶⁵ The FCC elaborated that "restrictions based on the availability of a central antenna will generally be permissible" if they meet the following conditions:

1. the person receives the fixed wireless service that the person desires and could receive with an individual antenna covered under the rule (*e.g.*, the person would be entitled to receive service from a specific provider, not simply a provider selected by the management entity);
2. the signal quality of the transmission to and from the person's leased space using the central antenna is as good as, or better than, the quality the person could receive or transmit with an individual antenna covered by the rule;
3. the costs associated with the use of the central antenna are not greater than the costs of installation, maintenance, and use of an individual antenna covered under the rule; and
4. the requirement to use the central antenna instead of an individual antenna does not unreasonably delay the person's ability to receive fixed wireless services.⁶⁶

⁶⁴ 47 C.F.R. § 1.4000(a)(3).

⁶⁵ *OTARD Order on Reconsideration*, 13 FCC Rcd at 18998 ¶ 86.

⁶⁶ *Id.* at 18999 ¶ 88. Although the FCC initially adopted the central antenna approach for video programming, it has extended this approach to fixed wireless services, such as Wi-Fi antennas. *Competitive Networks First Report and Order*, 15 FCC Rcd at 23027-28 ¶ 97-100; Federal Communications Commission, *Over-the-Air-Reception Devices Rule*, Information Sheet (July 2005), <http://www.fcc.gov/mb/facts/otard.html> (describing the central antenna approach as encompassing video programming and fixed wireless signals).

The central Wi-Fi antenna system at Logan meets all of these conditions.

A. Continental Would Have Access to Its Desired Service and Desired Service Provider

Continental could likely receive the same business services from the same provider using Logan's central Wi-Fi antenna system as it currently receives using the individual antenna installed in the Presidents Club. Although a primary concern of commenters in this docket is the right to choose a service provider,⁶⁷ Continental's preferential Presidents Club passengers have no rights under the OTARD rule.⁶⁸ Even if Continental's preferential passengers had OTARD rights, the central Wi-Fi antenna system offers them the same wireless Internet access service from a broader selection of Internet service providers than Continental.

1. Continental Employees

Continental employees could continue to receive the same services that they currently receive through the Presidents Club antenna. The *Supplemental Petition* provides scant information about the use of the Wi-Fi antenna other than to state that "employees traveling on business use this system to keep up with their business communications."⁶⁹ This language suggests that Continental's employees use wireless Internet service to access their corporate network. The central Wi-Fi antenna system at Logan provides managed services to support all wireless data users and applications, including wireless Internet access service, regardless of

⁶⁷ E.g., Comments of Charles E. Meacham, WT Docket No. 05-247 (Sept. 12, 2005) (filing Continental's form comments that ask the FCC to "ensur[e] the right of the public to use the wireless service of its choice"). Continental has reportedly sent an e-mail to its Presidents Club members, providing them with a set of form comments and encouraging them to file those comments in this proceeding. Glenn Fleishman, *Continental Urges Presidents Club Members to Write FCC*, Wi-Fi Net News, Aug. 18, 2005, <http://wifinetnews.com/archives/005603.html>. This e-mail would explain the hundreds of identical comments filed in this proceeding.

⁶⁸ See discussion *infra* at Section VI.F.

⁶⁹ *Supplemental Petition* at 3.

whether the user is a corporate or individual customer, WISP/ISP end user, or walk-up subscriber.

Continental could also likely receive service from its choice of providers. Although Continental neglected to disclose the identity of its service provider in the *Petition* or *Supplemental Petition*, its employees appear to use Fiberlink for remote access to the corporate network. According to Fiberlink's website, "Continental relies on network access to send and receive e-mail, tap into the company's Intranet and customer database, and access seat inventory and flight operations."⁷⁰ Continental reportedly "deployed Fiberlink's Extend360 in January 2003 to provide access for more than 1,500 employees in 150 cities."⁷¹ These descriptions are consistent with Continental's assertions in its *Supplemental Petition*, which states that employees use the Wi-Fi antenna "to keep up with their business communications."⁷²

Continental could continue to use Fiberlink to satisfy its remote access needs over the central Wi-Fi antenna system at Logan. As described above, AWG has deployed and operates a neutral host/common use wireless data system that accommodates subscribers from different service providers. One of the service providers on the central Wi-Fi antenna system, Boingo, has announced that Fiberlink is one of its partners and that Fiberlink's customers "now have one-click access to Boingo's industry-leading 18,000 Wi-Fi hot spots through Fiberlink's just-

⁷⁰ Fiberlink, Case Studies, http://www.fiberlink.com/system/modules/com.fiberlink.site/resources/FL_ConAir_CS-012105.pdf (last visited Sept. 26, 2005).

⁷¹ Elena Malykhina, *Remote Access Gets Easier: For Continental Airlines, Switching to a Remote-Access Service from Fiberlink Has Resulted in Substantial Cost Savings*, InformationWeek, May 10, 2005, <http://informationweek.com/story/showArticle.jhtml?articleID=163100679>.

⁷² *Supplemental Petition* at 3.

announced Extend360[®] service."⁷³ Thus, even though AWG provides the infrastructure for this central Wi-Fi antenna system, Continental could use Fiberlink for remote access.⁷⁴

2. Preferential Passengers

Even assuming, *arguendo*, that Continental's preferential passengers had OTARD rights, they could continue to receive the same services that they currently receive through the Presidents Club antenna. Continental's website indicates that preferential passengers who belong to the Presidents Club will have "[c]omplimentary high-speed wireless Internet access."⁷⁵ As mentioned above, the central Wi-Fi antenna system at Logan provides wireless Internet access service to corporate and individual customers, WISP/ISP end users, and walk-up subscribers.

These preferential passengers would also have a broader choice of Internet access service providers than is available from Continental. Although Continental has not disclosed any information about its Internet service provider, Continental appears to take service over a T-1 or DSL line and to transmit the signal over its Wi-Fi antenna to its preferential passengers as part of their Presidents Club membership fees. In other words, Presidents Club members receive

⁷³ Boingo Wireless, Case Studies, <http://www.boingo.com/partner/carrier9.html>.

⁷⁴ Although the existence of "free" wireless Internet access service in other airports is beyond the scope of this *Public Notice*, the sheer number of Boingo's hot spots, and the presence of Boingo hot spots in at least 96 airports in the United States, suggests that Continental could have similar arrangements at other airports. Boingo Wireless, <http://www.boingo.com/search.html?pgt=results&cnty=US&cte=Airport&bcct=96> (last visited Sept. 26, 2005).

⁷⁵ Continental Airlines, Presidents Club Amenities, <http://www.continental.com/travel/airport/lounge/amenities.asp?SID=3E6E87BB55034E728FB7216D316E25C4> (last visited Aug. 17, 2005).

wireless Internet access service from a single provider, *i.e.*, Continental, that resells the service of a single Internet service provider.⁷⁶

By contrast, the central Wi-Fi antenna system allows customers of hundreds of Internet service providers to receive wireless access to the Internet without paying additional charges or fees to AWG or Massport. AWG currently has two wireless Internet service providers ("WISPs") with roaming agreements, iPass and Boingo, on its central Wi-Fi antenna system and has entered into negotiations with three other national providers.⁷⁷ Anyone may gain secure Internet access "via a direct agreement with iPass or one of its more than 600 ISP or Value-Added Reseller partners,"⁷⁸ and Boingo has, or will soon have, agreements with several major service providers, including Earthlink, Fiberlink, BT Infonet, MCI, Telecom Italia, Nextel, and Skype.⁷⁹ Thus, if a Presidents Club member has an individual or corporate account with iPass, Boingo, or one of their affiliated ISPs or resellers, such as Fiberlink, the member could receive its choice of service providers over the central Wi-Fi antenna system.

⁷⁶ Continental's Wi-Fi antenna may also restrict access by its Presidents Club members to secure corporate networks. For example, Massport understands that iPass has entered into several agreements to provide secure connections from remote locations back to various corporate networks through a firewall. The individual corporations control which access points and networks their employees may use for this purpose, often limiting connections to iPass-enabled networks. Thus, while Continental's Wi-Fi antenna may preclude Presidents Club members from accessing their corporate networks through iPass, access through iPass is available to users of Logan's central Wi-Fi antenna system.

⁷⁷ Massport has no control over the negotiations with wireless Internet service providers.

⁷⁸ *Minneapolis Airport Gets Neutral-Host Wi-Fi*, m-Travel.com, Apr. 8, 2002, http://www.m-travel.com/news/2002/04/minneapolis_air.html.

⁷⁹ Boingo® Helps Major Brand Service Providers Get Into Wi-Fi Quickly and with Very Little Up Front Investment, <http://www.boingo.com/partner/carrier.html> (last visited Sept. 26, 2005).

B. The Central Wi-Fi Antenna System Provides Superior Signal Quality, Coverage, and Technical Support

The central Wi-Fi antenna system should provide Continental and its preferential passengers with a signal quality "as good as, or better than" the signal quality they would receive from the Wi-Fi antenna located in the Presidents Club. Although the FCC has apparently not interpreted the term "signal quality" in the context of the central antenna approach, it has suggested that a landlord should measure "acceptable signal quality" using the same unit of measurement as the petitioner, correctly position the equipment (*i.e.*, not merely position it to achieve maximum gain), and take measurements from the location of the proposed antenna.⁸⁰

An exact signal quality comparison is not possible because Continental did not go through the requisite permitting process with Massport and has not submitted any technical information in the record regarding its Wi-Fi antenna, even though it knew that Massport intended to rely upon the central antenna approach as a defense.⁸¹ Despite this absence of information, Logan's central Wi-Fi antenna system should provide identical or superior signal quality because it provides robust coverage throughout the airport. AWG designed this central Wi-Fi antenna system as a redundant, battery backed-up system to ensure high availability and quality of service for all users. AWG also has installed approximately 245 access points to provide full overlapping wireless coverage from the curb of the terminal to the tail of the airplane without any dead areas. This coverage area encompasses Terminals A, B, C, D, E, and Amelia Earhart, including the space that Continental leases for its Presidents Club. A third-party

⁸⁰ In re Lubliner, CSR 4915-O, *Order*, 13 FCC Rcd 4834, 4841 ¶ 20 (1997).

⁸¹ *Petition* at Exhibit C.

consultant recently confirmed the ubiquitous coverage of the central Wi-Fi antenna system, measuring strong (> -70 dBm) signal strength throughout most of the tested terminal areas.⁸²

When AWG initially deployed the central Wi-Fi antenna system, it tested the signal quality on the perimeter of the airport, in the common areas, and in the individual clubrooms, including the Presidents Club, and data throughput measured approximately 5 Mbps in most areas. AWG has deployed at least four access points that provide coverage to the Presidents Club and could easily deploy another access point within the Presidents Club. If a particular access point has several users associated with it, the central Wi-Fi antenna system can shift a new user to a less congested access point to ensure that data throughput remains acceptable for everyone.

The central Wi-Fi antenna system also has an elaborate network support structure in place to provide technical assistance and resolve any degradations in service quality. Although Massport understands that Continental may outsource the maintenance of its Wi-Fi system, the Logan's central Wi-Fi antenna system has four levels of on-site and off-site network support depending on the nature of the problem:

- **Level 1 Support.** For single user and end-user problems, the central Wi-Fi antenna system has on-site technicians available and an off-site call center available 24 hours a day, 7 days a week, and 365 days a year.
- **Level 2 Support.** For multiple-user problems, single access point problems, and sustained end-user problems, the central Wi-Fi antenna system has the same services available and also guarantees that an on-site technician will respond within two hours.
- **Level 3 Support.** For multiple user problems, multiple access point problems, router/switch/server problems, and sustained network problems, the central Wi-Fi antenna system has available an on-site technician, on-site network engineer (4-hour response), off-site network architect, off-site Cisco TAC support spare parts cache (next day parts replacement), and off-site call center.

⁸² *Engineering Audit* at 21, 23, 25, 27, attached as Exhibit B.

- **Level 4 Support.** For major network failures, multiple user problems, multiple access point problems, router/switch/server problems, and sustained network problems, the central Wi-Fi antenna system has available an on-site technician, on-site network engineer (4-hour response), off-site network architect (8-hour response), off-site executive/operations manager, and off-site Cisco TAC support spare parts cache (8-hour response and next day parts replacement), and off-site call center (24/7/365).

These technical support services may be reached via e-mail, telephone, and web and provide a high level of assurance that the superior signal quality of the central Wi-Fi antenna system will be available when users need it.

If Continental were to experience any problems with the signal strength or bandwidth availability of the central Wi-Fi antenna system that the network support personnel could not resolve, AWG could easily remedy the problem with minimal delay. A recent engineering audit has revealed that the central Wi-Fi antenna system provides a slightly weaker signal than Continental's Wi-Fi antenna in a corner of the Presidents Club.⁸³ AWG can improve signal quality in this specific area because it anticipated and planned for future growth in the design stage of the project, plotting an additional 240 access points around Logan to accommodate any users that require more capacity for bandwidth-intensive applications, such as streaming video. AWG estimates that it could add another access point in or near the Presidents Club, or any other tenant's exclusive area, within in one day. The installation of another access point would address this minor signal quality issue and increase the coverage and capacity of the central Wi-Fi antenna system. Thus, because of the ubiquitous coverage of the central Wi-Fi antenna system, Continental employees and preferential passengers should enjoy identical or superior signal quality with the added benefit of service that extends beyond the Presidents Club to all areas of Logan.

⁸³ *Id.* at 27.

C. The Central Wi-Fi Antenna System Is Likely to Be Less Expensive than Continental's Individual Antenna

Although Continental has provided no information about the cost of the Wi-Fi service in the Presidents Club, Massport believes a reasonable basis exists to conclude that the central Wi-Fi antenna system would be a less expensive alternative. In the *Petition* and *Supplemental Petition*, Continental disclosed nothing about the cost of its antenna, maintenance plan, service from the underlying Internet service provider, or any other costs associated with the Wi-Fi service in the Presidents Club. In a letter of July 5, 2005, Massport suggested that Continental could enter into an agreement with AWG for use of the central Wi-Fi antenna system.⁸⁴ Based on further research into Continental's particular situation, however, Massport believes that Continental would not need to contract with AWG but could use the central Wi-Fi antenna system at no additional charge from AWG or Massport, pursuant to Continental's existing agreement with Fiberlink.

In an affidavit, a Continental executive complained that "the costs associated with this alternative central antenna will unnecessarily and unreasonably be greater to Continental...."⁸⁵ As mentioned above, however, users that have an account with iPass, Boingo, or one of the hundreds of their affiliated ISPs, resellers, or other partners may access the central Wi-Fi antenna system without having to pay any additional charges to AWG or Massport. Because Continental employees appear to use Fiberlink for their remote access needs, and Fiberlink is a partner of Boingo, Massport believes Continental employees could continue to receive Wi-Fi service from Fiberlink as part of their existing service and without paying any extra fee to AWG or Massport.

⁸⁴ *Petition* at 4, Exhibit C.

⁸⁵ *Id.* at Affidavit in Support of Petition of Continental Airlines, Inc.

In fact, Continental would likely avoid certain costs because it would no longer have to take service from a separate Internet service provider in the Presidents Club.

Continental would also avoid having to pay maintenance costs for its antenna by taking service through the central Wi-Fi antenna system. As explained in Section II.B of these Comments, AWG is responsible for ensuring that the central Wi-Fi antenna system functions properly. The cancellation of Continental's maintenance account and removal of its antenna would further reduce the cost of providing its employees with remote access service.

Although Continental's preferential passengers who use the Presidents Club lounge have no right to "free" wireless Internet access service under the OTARD rule,⁸⁶ nothing would appear to prevent Continental from continuing to offer wireless Internet access service to these passengers as part of their membership dues to the Presidents Club. For example, Continental could purchase an account with Boingo or one of its partner service providers and allow its preferential passengers to access the Internet through the central Wi-Fi antenna system without paying AWG or Massport and without passing through the costs to its preferential passengers. Alternatively, the preferential passengers themselves could enroll with Boingo or one of its partners and receive Internet access service from any location in Logan's terminals, without having to pay AWG or Massport or to purchase a membership in the Presidents Club.⁸⁷

⁸⁶ While Continental has asked its Presidents Club members to submit a form e-mail to the FCC complaining about the loss of "free" Internet access service, Glenn Fleishman, *Continental Urges Presidents Club Members to Write FCC*, Wi-Fi Net News, Aug. 18, 2005, <http://wifinetnews.com/archives/005603.html>, the cost of service for these passengers is completely irrelevant under the OTARD analysis. The OTARD analysis inquires into the cost of the service for the *tenant* and not into the cost of the service for the *tenant's customers*. As explained in Section VI.A, *infra*, the FCC did not intend to extend the OTARD rule to resellers of services, such as Continental.

⁸⁷ Based on their published rates, a Continental passenger could purchase twelve months of Boingo service for less than the cost of an annual membership in the Presidents Club. *Compare* (continued...)

Finally, even though many commenters complain that Massport unlawfully seeks to charge them for the use of unlicensed spectrum,⁸⁸ these complaints are misguided. All passengers, tenants, employees, and visitors to Logan may use unlicensed devices on the 2.4 GHz band without having to pay anything. As mentioned above, anyone may access free information from www.loganwifi.com and www.massport.com over the wireless network regarding news, weather, flight and gate information, and local restaurants. Laptop and PDA users may also establish ad hoc networks over the unlicensed 2.4 GHz band, transmitting data among themselves without accessing the central Wi-Fi antenna system.⁸⁹ By contrast, users must have an individual or corporate agreement with an Internet service provider, or pay the daily rate, *only if* they want to connect to the *Internet*. An agreement or payment is necessary for Internet access service because it requires the cooperation of an Internet service provider. Thus, the use of unlicensed spectrum remains free for everyone, while wireless Internet access service requires a financial transaction.

D. Passengers and Continental Employees Would Experience No Delay in Receiving High-Speed Internet Access

The central Wi-Fi antenna system would also not unreasonably delay the provision of high-speed Internet access service to Continental or its preferential passengers. Although the

Boingo Wireless, www.boingo.com *with* Continental Airlines, Presidents Club Membership and Passbook Rates, <http://www.continental.com/travel/airport/lounge/rates.asp?SID=A0339FBC82464498B2629BC C192C06E6>.

⁸⁸ E.g., Comments of Marcus J. Lockard, ET Docket No. 05-247 (Aug. 22, 2005).

⁸⁹ Ad hoc networks will increase the noise heard by the central Wi-Fi antenna system, much like 2.4 GHz telephones and microwave ovens. Although ad hoc networks could theoretically turn a laptop or PDA into an access point, they present less of an interference problem than rogue access points because they do not support multiple connections and operate at lower power.

FCC expressed concern that unscrupulous landlords could require the removal of an individual antenna after merely announcing the intention of installing a central antenna,⁹⁰ a central Wi-Fi antenna system is already installed and operational at Logan. As mentioned above, AWG could also add access points to the central Wi-Fi antenna system in only one day. Because Continental and its preferential passengers already have access to high-speed Internet service through this system, the use of the central Wi-Fi antenna system would not delay their ability to receive such services. Thus, based on what Massport believes is a very reasonable and rational central Wi-Fi antenna approach, Massport may require Continental to remove the Wi-Fi antenna from its Presidents Club.

V. THE RESTRICTIONS ON CONTINENTAL'S ANTENNA ARE NECESSARY TO ACHIEVE LEGITIMATE SAFETY OBJECTIVES

The OTARD rule also permits the restriction of Continental's antenna because the proliferation of individual Wi-Fi antennas at Logan would interfere with the vital safety and security communications operating on the central Wi-Fi antenna system. In a letter to Continental, dated July 5, 2005, Massport outlined the safety and security concerns arising from interference already emanating from Continental's Wi-Fi antenna.⁹¹ Although section 1.4000 generally prohibits restrictions that impair installation, maintenance, and use of fixed wireless devices, it permits prior approval requirements and other restrictions that are necessary to accomplish "legitimate safety goals . . . that serve a stated purpose."⁹² To qualify for this safety exception, the restriction must satisfy four elements:

⁹⁰ *OTARD Order on Reconsideration*, 13 FCC Rcd at 18999 ¶ 89.

⁹¹ *Petition* at Exhibit C.

⁹² 47 C.F.R. 1.4000(b)(1); *In re Frankfurt*, CSR-5238-0, *Memorandum Opinion and Order*, 16 FCC Rcd 2875, 2886 ¶ 31 (2001); *OTARD Order on Reconsideration*, 13 FCC Rcd at 18969 ¶ 12, 18981 ¶ 41; *OTARD Report and Order*, 11 FCC Rcd at 19290 ¶ 24.

1. the legitimate safety objective of the restriction must be clearly defined;
2. the restriction must be necessary to accomplish the safety objective;
3. the restriction must be "no more burdensome to affected antenna users than is necessary to achieve" the defined safety objective; and
4. the restriction must be "applied to the extent practicable in a non-discriminatory manner to other appurtenances, devices, or fixtures that are comparable in size and weight and pose a similar or greater safety risk as those antennas to which local regulation would normally apply."⁹³

Massport satisfies each of these elements because the text of the Lease Agreement provides the safety objectives, and the restrictions are necessary to achieve these objectives, are not unduly burdensome to antenna users, and apply in a non-discriminatory manner to all existing or potential antenna users that present similar concerns. While Massport must restrict the use of individual Wi-Fi antennas to protect safety and security communications, it believes that a carefully managed central Wi-Fi antenna system could balance the public safety and commercial interests of the diverse group of users at Logan.

A. The Safety Objectives Are Clearly Defined in the Lease Agreement and Other Readily Available Documents

Section 1.4000(b)(1) of the FCC's rules requires the safety objective to be "either stated in the text, preamble, or legislative history of the restriction or described as applying to the restriction in a document that is readily available to antenna users."⁹⁴ The FCC has clarified that general lease provisions are sufficient "where the safety objective of a particular restriction is clearly apparent on the face of the restriction"⁹⁵ The FCC also permits property managers

⁹³ 47 C.F.R. 1.4000(b)(1).

⁹⁴ *Id.*

⁹⁵ In re Frankfurt, CSR-5238-O, *Memorandum Opinion and Order*, 16 FCC Rcd 2875, 2885 ¶ 30 (2001).

to "describ[e] the restriction and the clearly defined health or safety objective it is intended to promote[]" in a document that is readily available to antenna users."⁹⁶

The text of the Lease Agreement alerts Continental to the safety objectives associated with the use of the terminal. In particular, section 10.3 states that Continental:

shall not do or knowingly permit to be done anything which may interfere with the effectiveness or accessibility of any . . . communications system, key card access systems, . . . electrical system, fire-protection system, sprinkler system, alarm system, . . . installed or located on, under, in or adjacent to the Premises now or in the future.⁹⁷

The safety objective of this restriction appears in the text of the Lease Agreement and is also clearly apparent on the face of the provision. The lease provision protects the effectiveness and accessibility of vital utilities at Logan. Continental could reasonably have known that the installation and use of a radio transmitter could interfere with the communications systems at Logan. Continental should also have reasonably known that the additional cables or wiring from the Wi-Fi antenna could pose a risk to the electrical system in the terminal, especially because the complexity of terminal operations already requires dense wiring in the walls and ceilings.

The safety and security objectives also appear in other private documents that are "readily available" to Continental. For example, Massport and Continental amended the Lease Agreement on two occasions to reallocate a portion of the leased space to the TSA for baggage screening and a security checkpoint.⁹⁸ In addition, Massport and Continental entered into an Operating Agreement that contains confidential materials addressing the respective

⁹⁶ *OTARD Report and Order*, 11 FCC Rcd at 19292 ¶ 25.

⁹⁷ *Lease Agreement* § 10.3, attached as Exhibit A.

⁹⁸ Second Addendum to Terminal Lease by and between the Massachusetts Port Authority and Continental Airlines, Inc., L-7936(B) (Oct. 15, 2004), attached as Exhibit D; First Addendum to Lease, L-7936(A) (Apr. 13, 2004), attached as Exhibit E.

responsibilities of the parties and of first responders during an emergency situation. Massport has also provided Continental with an Emergency Procedures Manual for Logan. These private documents indicate that Continental had full knowledge of the unique safety and security issues associated with the airport environment.

Finally, the safety and security objectives are also evident in the pervasive federal regulation of airport security. As described in detail above, the federal government has imposed several safety and security responsibilities on Massport, as an airport operator, as well as on the TSA, Massachusetts State Police, Continental, and other airlines.⁹⁹ These statutes and regulations are public documents and are well known to all tenants, especially to Continental as the subject of many of the responsibilities.

B. The Antenna Restrictions Are Necessary to Achieve the Safety and Security Objectives

The lease restrictions are necessary to accomplish these legitimate safety objectives because the effectiveness and accessibility of the communications system are particularly important to the safety and security of airports in the post-9/11 world.

The central Wi-Fi antenna system at Logan provides numerous benefits that are an important adjunct to licensed radio systems. The installation of individual Wi-Fi antennas in the terminals would jeopardize these safety-related applications by creating interference and degrading the overall performance of the central Wi-Fi antenna system. A carefully managed central Wi-Fi antenna system avoids this interference without displacing either public safety or commercial users. The central Wi-Fi antenna system at Massport can accommodate all types of communications and can balance the interests of the respective users.

⁹⁹ *E.g.*, 14 C.F.R. pt. 139 (2005); 49 C.F.R. pts. 1542, 1544, and 1546.

1. The Central Wi-Fi Antenna System Can Provide Security and Reliability to Certain Public Safety Operations

The central Wi-Fi antenna system is important to the mission-critical and non-mission-critical communications of public safety agencies at Logan. Although public safety agencies have traditionally employed licensed private radio systems, the FCC's Wireless Broadband Access Task Force has recognized that "[w]ireless broadband technologies have the potential to benefit public safety entities across the country"¹⁰⁰ Because of these benefits, public safety entities "have begun to gravitate away from relying solely on their private networks."¹⁰¹ The central Wi-Fi antenna system provides public safety agencies at Logan with cost savings, enhanced functionalities, a secure network, and redundancy and reliability that is highly valued for carrying out their statutory responsibilities at Logan.

Public safety agencies receive cost savings from the central Wi-Fi antenna system. In a White Paper, submitted in an FCC proceeding on the future spectrum needs of emergency response providers,¹⁰² Dale Hatfield and Phil Weiser reported that public safety agencies "can increase productivity and cut costs by moving towards an integrated architecture" that includes PLMRS systems and other types of networks.¹⁰³ Hatfield and Weiser specifically recommended that "[i]n terms of developing an optimal network architecture, public safety agencies should also

¹⁰⁰ *Task Force Report* at 38.

¹⁰¹ Dale Hatfield and Phil Weiser, Taking a Fresh Look at Public Safety's Spectrum Needs: Toward a Next Generation Strategy for Public Safety Communications 14, attached to Letter from David S. Konczal, Mobile Satellite Ventures LP, to Marlene H. Dortch, Secretary, FCC, WT Docket No. 05-157 (June 17, 2005) [hereinafter *Hatfield/Weiser White Paper*].

¹⁰² The FCC initiated this proceeding in response to a statutory mandate "to assess short-term and long-term [spectrum] needs . . . for Federal, State, and local emergency response providers" Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 § 7502, 2004 U.S.C.A.N. (118 Stat. 3638, 3856) (2004).

¹⁰³ *Hatfield/Weiser White Paper* at 14.

be open to taking advantage of advances in wireless broadband technology developed for unlicensed spectrum," such as "wireless local area network (WLAN) technology (i.e., the 802.11 (WiFi) standard)." ¹⁰⁴ Massport has specifically gone in this direction in setting up a versatile and flexible communications system using licensed and unlicensed frequencies. The FCC has also observed that unlicensed spectrum permits public safety agencies "to enjoy savings that are typically limited to the high-volume commercial market." ¹⁰⁵ These economies of scale with respect to equipment purchases are especially vital for public safety agencies that must operate with limited budgets.

In addition, Logan's central Wi-Fi antenna system provides public safety agencies with enhanced functionalities for broadband applications. ¹⁰⁶ As mentioned above, the applications envisioned for use at Logan include (1) real-time, full-motion video from any location to any other location; (2) live video from an emergency scene to a command center; (3) accessing mug shots from the field; (4) mapping/location-based services; (5) digital image transfers; (6) large file transfers; and (7) bio-terrorism detection and response information. Public safety agencies require access to these data and video transmissions, while simultaneously engaging in voice communications. Because public safety operations in airports are highly mobile, this broadband access must also be mobile. ¹⁰⁷ The central Wi-Fi antenna system at Logan offers the enhanced

¹⁰⁴ *Id.*

¹⁰⁵ *Id.* at 15 (quoting News Release, FCC Improves Public Safety Access To The Latest Broadband Technology (Nov. 9, 2004)).

¹⁰⁶ The FCC's Wireless Broadband Access Task Force has noted that wireless broadband technologies "assist public safety officials in performing their jobs more efficiently and effectively in an environment that often requires immediate access to large amounts of information." *Task Force Report* at 38.

¹⁰⁷ Although the FCC has made spectrum in the 4.9 GHz band available for public safety operations, *In re the 4.9 GHz Band Transferred from Federal Government Use*, WT Docket No.

(continued...)

functionalities that public safety agencies need for their bandwidth-intensive applications. Thus, even though Massport has no control of the types of equipment or applications used by public safety agencies, the central Wi-Fi antenna system is available to them.

The central Wi-Fi antenna system enables public safety agencies at Logan to communicate over a secure network, which also gives them priority access in emergencies. While the FCC's Wireless Broadband Access Task Force acknowledged that "technological advances are enabling more secure wireless networks, safeguarding the confidentiality of the information transmitted over the network,"¹⁰⁸ some public safety agencies have complained that their private radio systems are susceptible to eavesdropping by users of radio scanners, potentially allowing such users to overhear sensitive information.¹⁰⁹ As mentioned above, the central Wi-Fi antenna system at Logan provides public safety users with secure virtual private networks and supports all technologically feasible encryption standards and protocols. The central Wi-Fi antenna system also affords priority treatment for safety and security communications across the entire network. Thus, as with wireline and wireless traffic,¹¹⁰ the prioritization and virtual private network technology will enable public safety agencies to share a

00-32, *Second Report and Order and Further Notice of Proposed Rule Making*, 17 FCC Rcd 3955 (2002), public safety organizations have noted that the available spectrum at 4.9 GHz is appropriate for short-range transmissions but is not particularly well-suited either for available mobile applications or for applications that require a signal to penetrate inside buildings. Joint Comments of National Public Safety Telecommunication Council and Association of Public-Safety Communications Officials-International, Inc., WT Docket No. 05-157, at 5 (Apr. 28, 2005).

¹⁰⁸ *Task Force Report* at 40.

¹⁰⁹ E.g., Jim Rendon, *Notebooks and Wi-Fi Keep Colorado Cops on the Beat*, SearchMobile Computing, Mar. 8, 2004, http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci953936,00.html.

¹¹⁰ 47 C.F.R. §§ 64.401, Appendix A, 64.402, Appendix B.

communications network with the general public without compromising their safety- and security-related operations.

Finally, the central Wi-Fi antenna system offers redundancy and reliability to public safety agencies. In the event of another 9/11, AWG could even enable public safety agencies to take over the entire network without concern that competing radio signals from other Wi-Fi networks would interfere. This would not be possible if several tenants operated Wi-Fi antennas in the close quarters at Logan. These precautions become invaluable in emergencies, such a 9/11 or a Katrina-type natural disaster.

The shortcomings of existing public safety communications networks have been well documented. The 9/11 Commission (1) found that the Fire Department of New York's ("FDNY") Private Land Mobile Radio Service ("PLMRS") system provided an "unreliable" means of transmitting information;¹¹¹ (2) concluded that the FDNY's PLMRS system "was simply overwhelmed by the number of units attempting to communicate on it,"¹¹² stating that "as many people tried to speak at once, their transmissions overlapped and often became indecipherable;"¹¹³ (3) observed that "NYPD [New York Police Department] radio communications became strained on most channels;"¹¹⁴ (4) cited the "Arlington County: After-Action Report" as reporting that "[a]lmost all aspects of communications continue to be problematic[,] . . . [c]ellular telephones were of little value[,] . . . [and] [r]adio channels were

¹¹¹ *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States* 301 (W.W. Norton & Company 2004).

¹¹² *Id.* at 322.

¹¹³ *Id.* at 301.

¹¹⁴ *Id.* at 309.

initially oversaturated;"¹¹⁵ and (5) noted that "[t]he 911 system was not equipped to handle the enormous volume of calls it received."¹¹⁶ The central Wi-Fi antenna system would be one way to relieve the oversaturation of the private and public telephone networks during emergencies by providing an alternative communications path for safety and security personnel at the airport.

The importance of reliable, redundant communications systems is also apparent in the aftermath of Hurricane Katrina. Kenneth Moran, the Director of the FCC's Office of Homeland Security, testified before the House Committee on Energy and Commerce that "[t]he damage to the communications infrastructure hampered the rescue operations of emergency responders."¹¹⁷ The media reported that "[t]he communications failures left many fire, ambulance and police officers with no way to communicate with their headquarters or each other at a time when thousands needed rescue and lawlessness was rampant."¹¹⁸ For example, hundreds of New Orleans police officers reportedly had to share a single frequency pair on a backup radio system,

¹¹⁵ *Id.* at 315.

¹¹⁶ *Id.* at 286.

¹¹⁷ Written Statement of Kenneth P. Moran, Director, Office of Homeland Security, Enforcement Bureau, Federal Communications Commission, on Hurricane Katrina, Committee on Energy and Commerce, U.S. House of Representatives 2, *available at* <http://energycommerce.house.gov/108/Hearings/09072005hearing1630/Moran.pdf>; Peter Grant & Christopher Rhoads, *After Katrina, Communications Still Hobbled*, Wall Street J., Sept. 8, 2005, at B3; Bruce Meyerson, *Phone Outages Still Widespread After Storm*, Associated Press (Aug. 31, 2005) ("Telephone outages persisted across Katrina's havoc-strewn path on Wednesday, frustrating people's efforts to locate family and friends and complicating rescue and relief operations."); Arshad Mohammed, *Telecom Damage Tops \$400 Million*, Wash. Post, Sept. 6, 2005, at D6 ("the storm damaged local police radio systems and made it much harder for emergency personnel to help those in need").

¹¹⁸ Peter Grant & Christopher Rhoads, *After Katrina, Communications Still Hobbled*, Wall Street J., Sept. 8, 2005, at B3.

which resulted in indecipherable communications and delayed the transmissions.¹¹⁹ The Mississippi National Guard relied on runners to communicate information among various commanders.¹²⁰

Although Hurricane Katrina caused hundreds of millions in damage to communications infrastructure,¹²¹ private Wi-Fi systems reportedly provided some of the most reliable forms of communication. "Users of Wi-Fi Internet services in New Orleans have been able to get messages out through temporary Internet services related to hospital or police networks, even as voice nets remain down for wireline and wireless customers."¹²² The central Wi-Fi antenna system at Logan could perform a similar function during an emergency situation, which is particularly important given Logan's status as a lynchpin in New England's transportation system. As mentioned above, the central Wi-Fi antenna system at Logan has several redundancies and safeguards, including an Uninterruptible Power Supply battery backup to protect from power outages and multiple wireline connections to the wireless Internet service providers.

2. Interference Would Adversely Impact Current and Proposed Safety and Security Applications

A number of entities with safety and security responsibilities at Logan currently use, are scheduled to start using, or are considering the use of the central Wi-Fi antenna system,

¹¹⁹ *Id.*; Bruce Meyerson, *Katrina Rescuers Improvise Communications*, Associated Press, Sept. 1, 2005.

¹²⁰ Bruce Meyerson, *Katrina Rescuers Improvise Communications*, Associated Press, Sept. 1, 2005.

¹²¹ Arshad Mohammed, *Telecom Damage Tops \$400 Million*, Wash. Post, Sept. 6, 2005, at D6 (noting that BellSouth estimated that its repairs alone will cost between \$400 million and \$600 million).

¹²² Loring Wirbel, *Storm of Controversy over Comms*, EE Times, Sept. 5, 2005, <http://www.eetimes.com/showArticle.jhtml?articleID=170700236>.

including the TSA, the Massachusetts State Police, and several airlines. The introduction of interference on the central Wi-Fi antenna system and the inability to reasonably control the overall RF operating environment would preclude or hinder these entities in the performance of their safety- and security-related responsibilities. The potential for interference could be minimized to everyone's benefit by limiting the installation of multiple, competing Wi-Fi systems which would not be under any central control. This solution would also balance the interests of multiple users by allowing public safety agencies to use the central Wi-Fi antenna system for security-related communications, while allowing other tenants to meet their Wi-Fi access needs in a reasonable manner.

TSA. The TSA was established in response to the events of 9/11 as part of the Aviation and Transportation Security Act ("ATSA"), which President George W. Bush signed into law on November 19, 2001. The ATSA requires the TSA to "be responsible for day-to-day Federal security screening operations for passenger air transportation and intrastate air transportation,"¹²³ while leaving access control primarily in the hands of Massport and other airport operators.¹²⁴ The TSA's responsibilities "include[] hiring, training, testing, and deploying or arranging for Federal security screeners, Federal security personnel, Federal law enforcement officers, and Federal Security Managers at U.S. airports."¹²⁵ The TSA also must "research, develop and

¹²³ Aviation and Transportation Security Act, Pub. Law 107-71 § 101(a), 115 Stat. 597, 597 (Nov. 19, 2001).

¹²⁴ *E.g.*, 49 C.F.R. § 1542.103; *see also* 49 C.F.R. § 1542.203 (security of AOA); *id.* § 1542.205 (airport identification media for security identification display area (SIDA)); *id.* § 1542.207 (access control system for secured areas); *id.* § 1542.209 (background checks for unescorted access to SIDA).

¹²⁵ Department of Transportation, Transportation Security Administration, Assumption of Civil Aviation Security Functions and Responsibilities Under Chapter 449, Title 49, U.S.C., 67 Fed. Reg. 7939, 7939 (Feb. 20, 2002).

deploy security equipment and programs at U.S. airports, coordinate transportation security intelligence information, coordinate transportation security efforts with Federal and State agencies, and deal with threats to transportation."¹²⁶ On February 17, 2002, the TSA assumed responsibility for certain elements of airport security,¹²⁷ such as passenger screening, and, on January 1, 2003, started screening all checked baggage at Logan for explosives.¹²⁸

In fulfilling these responsibilities safely and efficiently, the TSA is considering the integration of the central Wi-Fi antenna system into its communications system. As mentioned above, on July 18, 2005, the TSA instituted a pilot program to determine if it could use the central Wi-Fi antenna system at Logan to transmit communications between its security checkpoints and its central administrative office. Based on the success of this pilot program, the TSA plans to "explore other possible uses" of the central Wi-Fi antenna system.

Interference would threaten the effectiveness of the TSA's potential communications. If a tenant were to install an access point near a TSA checkpoint, the tenant's operations could interfere with the transmission of security-related data to and from the TSA offices at Logan. Specifically, the tenant's access point could interrupt the data transmission, meaning that the TSA agent would have to re-authenticate and retransmit the data. The TSA could also have to identify and move to a less congested channel. This interference risk is particularly important with respect to Continental's individual Wi-Fi antenna because a third-party consultant has

¹²⁶ *Id.*

¹²⁷ Aviation and Transportation Security Act, Pub. Law 107-71 § 101(g), 115 Stat. 597, 603 (Nov. 19, 2001); Department of Transportation, Transportation Security Administration, Assumption of Civil Aviation Security Functions and Responsibilities Under Chapter 449, Title 49, U.S.C., 67 Fed. Reg. 7939, 7939 (Feb. 20, 2002).

¹²⁸ *Financial Report* at 26.

documented degradation to the central Wi-Fi antenna system from Continental's individual Wi-Fi antenna near the TSA checkpoint in Terminal C.¹²⁹

State Police. The Massachusetts State Police is responsible for policing and security at all Massport properties, including Logan.¹³⁰ The safety and security of passengers and employees is so fundamental that the State Police has located a barracks on the airport grounds with specially trained officers who are responsible for enforcing TSA and Massport airport security rules and regulations, traffic laws, and other legal requirements. This particular barracks is one of only two United States police agencies certified by the International Association of Airport and Seaport Police.

State Troopers will start using the central Wi-Fi antenna system at Logan for communications related to airport safety and security in the near future. As mentioned above, the State Police will deploy iPAQ devices on the central Wi-Fi antenna system for the transmission and reception of traffic enforcement data and for mobile access to images and data throughout the airport. Although the State Police conduct certain security-related operations on licensed spectrum, these iPAQ devices are the only technology certified for use by the state and national data repositories. The State Police also considering the use of a remote-controlled robot in conjunction with the central Wi-Fi antenna system.

As with the TSA, interference from unauthorized access points would seriously degrade the State Police's planned reliance on the central Wi-Fi antenna system. State Troopers present a slightly different situation than the TSA checkpoint because they must move between terminals while sending and receiving transmissions. If a State Trooper passes too close to an

¹²⁹ *Engineering Audit* at 15, 30, 31, attached as Exhibit A.

¹³⁰ Chapter 274 of the Act of 1959 (codified at Mass Gen. Laws ch. 22 (2005)).

unauthorized access point, the iPAQ device will drop the existing connection in favor of the unauthorized access point with a stronger signal. The iPAQ device must re-authenticate and pick up the transmission again, which could prevent the State Trooper from having the most up-to-date information before addressing the security issue.

Airlines. The TSA has promulgated regulations for aircraft operators to accept and screen baggage and cargo.¹³¹ As discussed in greater detail above, British Airways, Virgin Atlantic, and United Airlines currently use the central Wi-Fi antenna system for baggage reconciliation. The central Wi-Fi antenna system permits airlines to track baggage throughout the airport using handheld devices that are on a seamless private virtual local area network.

Interference could disrupt the use of the Wi-Fi backbone for baggage reconciliation by the airlines. As mentioned above, if every tenant had an individual antenna, the cumulative interference would reduce operational efficiency for these mobile devices. This loss of efficiency could require airlines to check and re-check bags multiple times or even cancel or delay a flight in order to pull bags off a loaded plane. An airline could also not replicate the central Wi-Fi antenna system's coverage with an individual antenna because the airline could not place access points in common areas, such as the ramp.

C. Massport Narrowly Tailored Its Restrictions

Section 10.3 of the Lease Agreement is "no more burdensome to affected antenna users than is necessary to achieve" the defined safety and security objectives, even though it covers all potential modifications to Continental's leased space.¹³² This general prohibition on the installation of individual antennas is not overly burdensome because Massport allows its tenants

¹³¹ 49 C.F.R. §§ 1544.203, 1544.205, 1546.203, 1546.205.

¹³² *Lease Agreement* § 10.3, attached as Exhibit A.

to (1) use the central Wi-Fi antenna system, or (2) request an exemption through the prior approval process.¹³³

The FCC has recognized that lease restrictions will not constitute an impairment if a central antenna is available and meets four specific conditions.¹³⁴ In a letter dated July 5, 2005, Massport notified Continental of the applicability of the central antenna approach.¹³⁵ As described in Section IV of these Comments, the central Wi-Fi antenna system meets these four conditions because it provides Continental with the same wireless Internet access service, broader choice of provider, identical or superior signal quality, comparable cost structure, and no unreasonable delays.

The Lease Agreement also allows Continental to request permission to install its own Wi-Fi antenna through a prior approval process, which is described in the letters from Massport to Continental of June 10, 2005, and July 5, 2005.¹³⁶ The FCC has repeatedly recognized that prior approval restrictions are permissible if they are for a safety-related purpose.¹³⁷ As mentioned above, Section 9.8 of the Lease Agreement allows Continental to "submit a complete Tenant Alteration Application ("TAA")" to propose the placement of communications equipment in the Presidents Club.¹³⁸ Although Continental claims that the TAA process "is really applicable to 'construction' done to the Premises,"¹³⁹ the plain language of the Lease Agreement indicates

¹³³ *E.g., id.* §§ 7.1(a)(xi), (xii); 7.2; 9.4; 9.7; 9.8.

¹³⁴ *OTARD Order on Reconsideration*, 13 FCC Rcd at 18999 ¶ 88.

¹³⁵ *Petition* at Exhibit C.

¹³⁶ *Id.* at Exhibit A, Exhibit C.

¹³⁷ *E.g., In re Frankfurt*, CSR-5238-0, *Memorandum Opinion and Order*, 16 FCC Rcd 2875, 2886 ¶ 31 (2001).

¹³⁸ *Lease Agreement* § 9.8, attached as Exhibit A.

¹³⁹ *Supplemental Petition* at 5.

otherwise. Section 9.4 states that "[t]he Tenant shall not *place* or construct any improvements, structures, alterations, modifications, signs, *communications equipment*, *wiring* or additions in, to, or upon the Premises without prior written approval" ¹⁴⁰ Because the installation of Continental's Wi-Fi antenna involved the placement of communications equipment in the Presidents Club, and the Wi-Fi antenna is presumably connected by wire to a T-1 or DSL line, the TAA process would apply to this situation. Continental never took advantage of this lease provision to request prior approval of its individual Wi-Fi antenna.

D. The Restrictions Apply in a Nondiscriminatory Manner

The safety and security restrictions apply equally to all tenants at Logan. Section 1.4000(b)(1) requires the landlord or management entity to apply the safety restriction "to the extent practicable in a non-discriminatory manner to other appurtenances, devices, or fixtures that are comparable in size and weight and pose a similar or greater safety risk as these antennas" ¹⁴¹ This utilities provision applies in a non-discriminatory manner to all tenants because it constitutes part of every Lease Agreement that Massport has negotiated with every tenant at Logan. Each tenant also has the opportunity to use the central Wi-Fi antenna system or to request permission to install its own antenna under the TAA process.

Continental and several commenters suggest that Massport may not apply the safety restrictions in a nondiscriminatory manner. ¹⁴² Although the precise locations and operators of unauthorized Wi-Fi access points is difficult to determine, Massport has attempted to enforce the utilities provision in its lease agreements as fairly as possible. The central Wi-Fi antenna system

¹⁴⁰ *Lease Agreement* § 9.4 (emphasis added), attached as Exhibit A.

¹⁴¹ 47 C.F.R. § 1.4000(b)(1).

¹⁴² *Supplemental Petition* at 8; e.g., Comments of Jonathan Goler, ET Docket No. 05-247 (Aug. 22, 2005); Comments of Robert D. Gordon, ET Docket No. 05-247 (Aug. 17, 2005).

is distinguishable because, unlike Continental, AWG acquired prior approval to install its approximately 245 access points throughout Logan. Even if AWG had not acquired prior approval, Massport could treat it differently because, unlike Continental, AWG carries the very safety and security communications that require protection from interference and designed its system to avoid causing interference to such communications. Thus, the central Wi-Fi antenna system would not pose a similar interference risk as the Continental Wi-Fi antenna.

VI. THE OTARD RULE SHOULD NOT APPLY TO CONTINENTAL'S WI-FI ANTENNA

As discussed above, Massport's central Wi-Fi antenna system fits within two clearly defined exceptions to the OTARD rule. However, the OTARD rule may not govern the installation and use of Continental's individual Wi-Fi antenna because Continental either resells commercial wireless Internet access service or does not receive or transmit a commercial non-broadcast communications signal. The OTARD rule should also not apply because Continental does not use its Wi-Fi antenna to communicate with a fixed wireless service provider outside of Continental's Presidents Club, Logan is a governmental facility, and Presidents Club members have no rights under the rule as non-tenants.

A. Continental Is Not Covered by the OTARD Rule as a Reseller of Wireless Internet Access Service

Continental has no right to install and use a Wi-Fi antenna because the OTARD protections apply only to customer-end antennas and not to antennas used to resell wireless Internet access service to third parties. In an *Order on Reconsideration*, the FCC stated that "to invoke the protections of the OTARD rule, the equipment *must be installed in order to serve the*

customer on such premises . . ."¹⁴³ The FCC also clarified that "the OTARD protections would apply to installations serving the premises customer that also relay signals to other customers . . . but would not apply to installations that are designed *primarily* for use as hubs for distribution of service" ¹⁴⁴

The record in this docket indicates that the Wi-Fi antenna was not installed to serve the premises customer, *i.e.*, Continental, but was instead installed to serve Continental's preferential passengers. In the *Petition*, and in a letter to Massport dated June 23, 2005, Continental stated that it provides wireless Internet service "to its customers at the President's Club."¹⁴⁵ In the *Supplemental Petition*, Continental amended its assertion to include employees but still indicated that "the wireless service in our Presidents Club is *primarily* a service offered free of charge to our frequent flyer customers who are members of the Club."¹⁴⁶ To join the Presidents Club, passengers must purchase a book of individual passes or an annual, three-year, or lifetime membership.¹⁴⁷ Although Continental touts its wireless Internet service as "free," it appears to refer to Presidents Club members as "revenue customers."¹⁴⁸ Several Presidents Club members also have filed comments in this proceeding noting that they indirectly "pay for the [I]nternet

¹⁴³ In re Promotion of Competitive Networks in Local Telecommunications Markets, WT Docket No. 99-217, *Order on Reconsideration*, 19 FCC Rcd 5637, 5644 ¶ 17 (2004) [hereinafter *Competitive Networks Order on Reconsideration*].

¹⁴⁴ *Id.* at 5644 n.42 (emphasis added).

¹⁴⁵ *Petition* at 3, Exhibit B.

¹⁴⁶ *Supplemental Petition* at 2 (emphasis added).

¹⁴⁷ Presidents Club Membership & Passbook Rates, <http://www.continental.com/travel/airport/lounge/rates.asp?SID=8B9F0BE0885E4CD09E288E51E5F9311A> (last visited Aug. 18, 2005). While a book of ten individual passes costs \$250 (or \$25 a pass), a standard annual membership costs \$375 per year plus a \$50 new member initiation fee. *Id.*

¹⁴⁸ *Supplemental Petition* at 3.

through our dues."¹⁴⁹ Thus, because Continental limits "free" wireless Internet access service to passengers who purchase Presidents Club memberships, it appears to act as a reseller of wireless Internet access service rather than as a premises customer of such a service.

Although Continental attempts to fit within the OTARD rule by claiming that its own employees use the wireless Internet access service in the Presidents Club, it has not provided sufficient evidence of this fact. As mentioned above, "the OTARD protections apply to installations serving the premises customer that also relay signals to other customers" but not "to installations that are designed primarily for use as hubs for distribution of service."¹⁵⁰ In the *Supplemental Petition*, Continental concedes that "the wireless service in our Presidents Club is *primarily* a service" for preferential passengers.¹⁵¹ This admission suggests that Continental's Wi-Fi antenna is actually a hub for the distribution of service and does not qualify for the OTARD protections.

Continental claims that the wireless Internet access service "is also routinely used by our employees who are members of the Presidents Club or otherwise [are] allowed access."¹⁵²

Although Continental implies that its employees receive wireless Internet access service without

¹⁴⁹ Comments of Col. George Wolf (Aug. 16, 2005); *see e.g.*, Comments of Denis M. Wolowiecki, ET Docket No. 05-247 (Aug. 23, 2005) ("As a dues paying member of the lounges, this is a service that I have paid for."); Comments of D. Tim Markovich, ET Docket No. 05-247 (Aug. 18, 2005) ("I pay an annual membership fee, which includes wireless access when I am in a Presidents [sic] Club."); Comments of David Mitchell, ET Docket No. 05-247 (Aug. 17, 2005) ("I consider that part of my several hundred dollars per year membership fee covers wireless network access."); Comments of Bryan White, ET Docket No. 05-247 (Aug. 17, 2005) ("They may look at this as if it is free but if [sic] is just a portion of the annual [sic] fee we pay for this service"). Because Continental incorporates the charges for wireless Internet access service into the Presidents Club membership dues, the only travelers who actually receive this service for free are those who pirate Continental's signal by loitering outside of the Presidents Club.

¹⁵⁰ *Competitive Networks Order on Reconsideration*, 19 FCC Rcd at 5644 ¶ 17 n.42.

¹⁵¹ *Supplemental Petition* at 2 (emphasis added).

¹⁵² *Id.* at 3.

having to join the Presidents Club,¹⁵³ a Continental flight attendant filed comments in this docket reporting that he has to pay a "membership fee" to use this service.¹⁵⁴ Continental further concedes that it has no records identifying the use of the wireless Internet access service by non-paying employees.¹⁵⁵ Thus, despite its assertions, Continental has failed to establish itself as a "premises customer" of the wireless Internet access service, nor has it even identified the provider of its wireless Internet access service, and, therefore, may not take advantage of the OTARD rule.

Even if Continental could prove that it is a "premises customer," the OTARD rule would not cover the resale of that service to its preferential passengers. The underlying purpose of the OTARD rule is to allow homeowners or tenants to install an antenna in order to purchase service from their choice of providers and not to allow commercial providers to extend their businesses. While the FCC stated that "the OTARD protections would apply to installations serving the premises customer that also relay signals to other customers,"¹⁵⁶ it noted that it "do[es] not intend that carriers may simply locate their hub-sites on the premises of a customer in order to avoid compliance with a legitimate zoning regulation."¹⁵⁷ Assuming that Continental takes service from a wireless Internet service provider as a premises customer, the OTARD rule would arguably permit the Internet service provider to install an antenna to provide service to

¹⁵³ *Id.*

¹⁵⁴ Comments of Robert A. Waldrip, ET Docket No. 05-247 (Aug. 17, 2005).

¹⁵⁵ "Revenue and non-revenue customers are not separately tracked such that Continental would be able to differentiate between its users of the wireless system" *Supplemental Petition* at 3. Although Continental's General Manager at Logan estimates that half of the users of the wireless Internet access service are employees, *id.*, the *Supplemental Petition* contains no indication that these employees are not dues-paying members of the Presidents Club.

¹⁵⁶ *Competitive Networks Order on Reconsideration*, 19 FCC Rcd at 5644 ¶ 17 n.42.

¹⁵⁷ *Id.* at 5644 ¶ 17.

Continental and to each of the Presidents Club members with whom it has a direct agreement. But the OTARD rule would not permit a tenant, such as Continental, to resell this high-speed wireless Internet access service out of its leased space.

If the FCC were to interpret the OTARD rule to allow the installation and use of any RF-generating device at any location, landlords would lose control over the management of their properties. A tenant could establish any type of business for which it could demonstrate the use of a wireless device in its operation, regardless of lease terms designating the property as a residential or a special-use facility. On the other hand, if Continental were now to argue that it provides a "commercial fixed wireless service" to its preferential passengers, it would be in violation of the OTARD rule. Continental would also be in violation of its Lease Agreement with Massport because the provision of a commercial communications service is not one of the authorized activities.

B. The OTARD Rule Applies Only to Fixed Wireless Devices Used to Receive "Commercial" Non-Broadcast Communications Signals

Section 1.4000(a)(2) of the FCC's rules defines "fixed wireless signals" to mean "any commercial non-broadcast communications signals transmitted via wireless technology to and/or from a fixed customer location."¹⁵⁸ Based on this definition, the FCC has limited the OTARD protections to fixed wireless service customers who receive a *commercial* wireless signal, and has not applied the OTARD protections to individuals who receive a *non-commercial*, or "*free*," wireless signal.

The OTARD rule would not permit the installation and use of the Wi-Fi antenna in the Presidents Club because Continental has not alleged that it uses the antenna to receive or

¹⁵⁸ 47 C.F.R. § 1.4000(a)(2).

transmit commercial fixed wireless service. Specifically, Continental has not claimed that it uses the antenna to receive Internet access service in the Presidents Club from a commercial wireless Internet service provider. Because Continental likely receives Internet access service over a T-1 or DSL line and uses the Wi-Fi antenna merely to relay the signal within the Presidents Club, Continental's Wi-Fi antenna is not involved in the reception of a commercial fixed wireless service. Thus, because Continental does not appear to use the Wi-Fi antenna to receive commercial fixed wireless service, it has no right under the OTARD rule to install a Wi-Fi antenna for the use of its employees or preferential passengers.

The FCC has previously refused to preempt private lease restrictions on the installation of antennas for voluntary, non-commercial service, such as Continental's wireless Internet access service. In 2001, the FCC declined to preempt private agreements restricting the installation of antennas used for Amateur Radio Service communications.¹⁵⁹ The petitioners argued that the FCC had preempted private agreements in the OTARD context and should not discriminate against amateur radio operators.¹⁶⁰ Although the FCC recognized that "there is a strong federal interest in promoting amateur radio communications,"¹⁶¹ it stated that the FCC "does not exercise its preemption power lightly, and employs this power only as necessary to carry out the provisions of the Communications Act."¹⁶² The FCC found that the statutory goals of promoting telecommunications competition and encouraging commercial deployment of new

¹⁵⁹ In re Modification and Clarification of Policies and Procedures Governing Siting and Maintenance of Amateur Radio Antennas and Support Structures, and Amendment of Section 97.15 of the Commission's Rules Governing the Amateur Radio Service, RM-8763, *Memorandum Opinion and Order*, 17 FCC Rcd 333, 337 ¶ 9 (2001), *recon. denied*, 17 FCC Rcd 19408 (2002).

¹⁶⁰ *Id.* at 335 ¶ 7.

¹⁶¹ *Id.* at 335 ¶ 5.

¹⁶² *Id.* at 335-36 ¶ 7.

telecommunications technologies were not applicable because the Amateur Radio Service is a voluntary noncommercial service.¹⁶³ The FCC further noted that it would not preempt private agreements because "there are other methods amateur radio operators can use to transmit amateur service communications that do not require an antenna installation at their residence."¹⁶⁴

Just as the FCC declined to subject the Amateur Radio Service to the OTARD rule, the FCC should deny Continental's Petition for Declaratory Ruling. In particular, Continental entered into a voluntary agreement with Massport to lease space in Terminal C at Logan. The objectives of the Communications Act would not be furthered by preempting this private lease restriction because Continental offers a non-telecommunications, noncommercial service over its individual Wi-Fi antenna. Finally, Continental employees have several alternatives to receive Internet access service that do not require the installation of an antenna in the Presidents Club, such as using the central Wi-Fi antenna system or wired service.¹⁶⁵ Thus, the FCC should not exercise its preemption authority to invalidate the lease restriction on Continental's use of an individual Wi-Fi antenna in the Presidents Club.

C. The OTARD Rule Applies Only to Signals Originating or Terminating Outside of a Lessee's Exclusive-Use Premises

The OTARD rule provides no protection for antennas installed and used only for transmission and/or reception of signals originating within a lessee's exclusive-use premises. Because Continental has not intended for its Wi-Fi antenna to receive or transmit fixed wireless

¹⁶³ *Id.* at 336 ¶ 7.

¹⁶⁴ *Id.* at 335 ¶ 6, 336 ¶ 7.

¹⁶⁵ *E.g.*, Comments of Michael Kramer, ET Docket No. 05-247 (Aug. 3, 2005) ("Continental has always offered free Internet access in their clubs, but it used to be via a phone connection which allowed you to dial from a laptop.").

signals to a commercial service provider outside of the Presidents Club, the OTARD rule would not authorize the installation and use of that antenna.

The FCC has repeatedly indicated that the intent of the OTARD rule is to permit lessees to install and use antennas that are necessary to receive and transmit signals originating or terminating outside of the exclusive-use premises. In the *Second Report and Order*, the FCC concluded that the OTARD rule will permit renters to "install Section 207 reception devices wherever they rent space outside of a building, such as balconies, balcony railings, patios, yards, gardens, or any other similar areas."¹⁶⁶ The FCC further explained that the OTARD rule will allow "the installation of Section 207 devices inside rental units and anticipates the development of future technologies that will create devices capable of receiving video programming signals inside buildings."¹⁶⁷

This language demonstrates that the intent of the OTARD rule is to permit the premises customer to receive signals from outside the premises through the installation of an antenna outside the premises, if the tenant has rights to outside facilities, or inside the premises, if the tenant does not lease any space outside of the building. In other words, a wireless access point used only for an in-premises LAN is not a "Section 207 device" because it is not needed by the tenant to receive or transmit communications signals of a commercial provider originating or terminating outside the premises.

Even when the FCC extended the OTARD rule to fixed wireless services, it based its decision on the need for a customer to receive services from outside of its exclusive-use

¹⁶⁶ In re Implementation of Section 207 of the Telecommunications Act of 1996; Restrictions on Over-the-Air Reception Devices: Television Broadcast, Multichannel Multipoint Distribution and Direct Broadcast Satellite Services, CS Docket No. 96-83, *Second Report and Order*, 13 FCC Rcd 23874, 23875 ¶ 2 [hereinafter *Second Report and Order*].

¹⁶⁷ *Id.* at 23875-76 ¶ 2.

premises. The FCC did not grant customers the right to operate wireless devices generally on leased premises. To the contrary, the FCC declined to extend the OTARD rule to the operation of "hub or relay antennas used to transmit signals to and/or receive signals from multiple customer locations."¹⁶⁸ Although the FCC subsequently permitted the use of point-to-point-to-point and mesh architectures, it limited the OTARD rule to "any customer-end device that would have been covered by our rules were it not for the devices' routing/relaying functionality."¹⁶⁹ Thus, the FCC restricted the applicability of the OTARD rule to customer-end antennas that receive or transmit signals to or from a commercial provider located outside of the lessee's exclusive-use premises.

Continental has apparently not installed its Wi-Fi antenna to receive fixed wireless signals from outside of the Presidents Club or to transmit such signals to a third-party service provider outside of the Presidents Club. As mentioned above, Continental has not alleged that it receives wireless Internet access service in the Presidents Club from a wireless Internet service provider located outside the Presidents Club. Continental likely receives Internet access service over a T-1 or DSL line and uses the Wi-Fi antenna only to create a wireless LAN within the Presidents Club. Continental also does not transmit signals to a third-party service provider outside of the Presidents Club. Thus, because Continental's Wi-Fi antenna is not used so that Continental can communicate with a third-party wireless service provider outside of the Presidents Club, the OTARD rule would not authorize the installation and use of that antenna.

¹⁶⁸ *Competitive Networks First Report and Order*, 15 FCC Rcd at 23028 ¶ 99.

¹⁶⁹ *Competitive Networks Order on Reconsideration*, 19 FCC Rcd at 5644 ¶ 18.

D. The FCC Has Never Enforced the OTARD Rule Against a Governmental Entity or Facility

The OTARD rule should not apply to a governmental entity that has restricted the installation and use of antennas as part of its responsibility for managing a sensitive governmental facility, such as Logan. None of the FCC's orders appear to enforce the OTARD rule in a governmental building, and the FCC has openly questioned the applicability of competitive access requirements in general for airports. Specifically, in a *Further Notice of Proposed Rulemaking* regarding competitive telecommunications carrier access to multiple tenant environments, the FCC asked if "a nondiscriminatory access rule [is] appropriate . . . at municipal airports, in which a local government often leases space to various commercial retail establishments."¹⁷⁰ The FCC has yet to resolve this issue, even though the *Further Notice* has remained pending for almost five years. The applicability of the OTARD rule is even more questionable where, as at Logan, the governmental building already meets the rule's underlying goal of competition and customer choice.

E. The FCC Should Grant Airports the Same Exemption from OTARD that It Has Granted to Other Special-Use Facilities

If, despite the foregoing, the FCC concludes that the OTARD rule applies to Continental's situation, the FCC should include airports in its exemption of special-use facilities from the OTARD rule. In a *Second Report and Order*, the FCC exempted college and university dormitories from the OTARD rule after finding that campus housing is unlike most residential rental arrangements. In particular, the FCC concluded that

no one has shown that a university has the same relationship to a dormitory resident as a landlord to a tenant, that a dormitory room is a leasehold, that landlord-tenant law applies equally to dormitories, or that the practical problems

¹⁷⁰ *Competitive Networks First Report and Order*, 15 FCC Rcd at 23049-50 ¶ 152.

associated with extending our rules to leaseholds can be similarly resolved with respect to dormitories¹⁷¹

Although the FCC retains the exclusive authority to govern RF interference, it permits colleges and universities to limit devices placed or used on their property.

The FCC should specifically exempt airports from the application of the OTARD rule, just as it has with college and university dormitories. Airport tenants have similarly limited rights and, of necessity, do not enjoy the same latitude in using their premises as tenants in a residential or commercial office building. As explained in these Comments, Massport exercises significant control over terminal facilities at Logan through its leasing arrangements with airlines and other tenants to satisfy its safety, security, and overall management responsibilities. In the Lease Agreement, Massport and Continental even agreed that Continental would use the leased space only for certain enumerated purposes. Operation of a wireless LAN for the convenience of its preferential passengers is not among these rights.

F. Presidents Club Members Have No Rights Under the OTARD Rule

The OTARD rule grants no protections to Presidents Club members. Section 1.4000 applies to antennas placed "on property within the exclusive use and control of the antenna user where the user has a direct or indirect ownership or leasehold interest in the property"¹⁷² As the primary users of the Wi-Fi antenna in the Presidents Club, Continental's preferential passengers may not assert OTARD rights because they fail to satisfy either component of this requirement.

Preferential passengers have no "direct or indirect ownership or leasehold interest" in the Presidents Club. As an initial matter, these passengers lack direct leasehold interests because

¹⁷¹ *Second Report and Order*, 13 FCC Rcd at 23889 ¶ 29 n.73.

¹⁷² 47 C.F.R. § 1.4000(a)(1).

they have not entered into individual lease agreements with Massport. These passengers also lack indirect leasehold interests. Although the FCC has extended OTARD rights to the father of a homeowner who resided on the property and had a power of attorney to act on behalf of his son,¹⁷³ it has never permitted mere *customers* of a tenant to exercise such rights. Continental has also not conferred its leasehold interest on its preferential passengers. Section 16.1 of the Lease Agreement states that "[t]enant shall not . . . sublet the Premises or any part thereof or allow the same to be used or occupied by others . . . without, in each instance, obtaining the prior written approval of the Authority."¹⁷⁴ Because Continental has not followed the requisite procedures for obtaining Massport's prior written approval for a sublet of the Presidents Club,¹⁷⁵ the preferential passengers have not obtained an indirect leasehold interest in the Presidents Club. Even if the preferential passengers had an indirect leasehold interest in the Presidents Club by virtue of paying their membership dues, they would still be subject to the provisions of the Lease Agreement prohibiting the installation of Wi-Fi antennas without prior approval.¹⁷⁶

The OTARD protections also should not apply to Continental's preferential passengers because they lack "exclusive use and control" of the Presidents Club. Although Continental has the right to exclude non-members from the Presidents Club, no individual member has the exclusive right to permit or deny access to the Presidents Club. Thus, members of the Presidents Club have no rights under the OTARD rule.

¹⁷³ In re Roberts, CSR 5531-0, *Memorandum Opinion and Order*, 16 FCC Rcd 10972, 10977 ¶ 11 (2001).

¹⁷⁴ *Lease Agreement* § 16.1, attached as Exhibit A.

¹⁷⁵ Section 16.2 establishes conditions of subletting property at Logan, including the assumption of all obligations under the Lease Agreement and the payment of additional rent. *Id.* § 16.2.

¹⁷⁶ *Id.*

VII. THE FCC EXCEEDED ITS STATUTORY AUTHORITY IN APPLYING THE OTARD RULE TO WI-FI ANTENNAS

Even if Continental were using its individual Wi-Fi antenna to receive a fixed wireless service, which it is not, the FCC lacked the statutory authority to extend the OTARD rule to fixed wireless signals. As an initial matter, Congress specifically limited the FCC's authority to the promulgation of rules that would enable viewers to receive video programming services. Although the FCC claimed to have the ancillary jurisdiction to extend the OTARD rule to the transmission and reception of fixed wireless signals, it lacks general jurisdiction over the installation of fixed wireless antennas.

A. Congress Expressly Limited the FCC's Authority

In 1996, Congress authorized the FCC to regulate restrictions on over-the-air-reception devices. In particular, section 207 of the Telecommunications Act of 1996 directed the FCC to "prohibit restrictions that impair a viewer's ability to receive video programming services through devices designed for over-the-air reception of television broadcast signals, multichannel multipoint distribution service, or direct broadcast satellite services."¹⁷⁷ The legislative history referred only to protecting a viewer's ability to use an antenna "designed for off-the-air reception of television broadcast signals or of satellite receivers designed for receipt of [direct broadcast satellite] services."¹⁷⁸ Because Congress limited the FCC's authority to promulgate rules to reception devices and video programming services, the extension of those rules to the transmission and reception of fixed wireless signals violated the textual boundaries of this specific statutory provision.

¹⁷⁷ Telecommunications Act of 1996, Pub. L. 104-104 § 207, 110 Stat. 56, 114 (1996).

¹⁷⁸ H.R. Rep. No. 104-204, at 124 (1995), *reprinted in* 1996 U.S.C.C.A.N. 10, 91.

Despite the plain language of section 207, the FCC asserted that it possesses the substantive authority to extend the OTARD rule to fixed wireless signals under section 303(r) of the Communications Act. In the *First Report and Order*, the FCC claimed that section 207 "reflects Congress' recognition that . . . the Commission has always possessed authority to promulgate rules addressing OTARDs" because that statutory provision authorizes the promulgation of regulations "pursuant to section 303."¹⁷⁹ But section 303(r) is a procedural provision that authorizes the FCC to adopt regulations "necessary to carry out the provisions of this chapter" and is not an independent source of delegated authority.¹⁸⁰

The FCC stated that section 207 merely created a timing deadline for the substantive authority under section 303(r) because it required the promulgation of the OTARD rule "[w]ithin 180 days."¹⁸¹ If section 303(r) already provided the FCC with the authority to extend the OTARD rule to services other than those listed in section 207, then all of section 207, except for the three-word introductory clause regarding the timing of the rulemaking, was extraneous language. This interpretation of the statute would contradict the basic principle of statutory construction not to deny effect to any part of a statute's language.¹⁸²

¹⁷⁹ *Competitive Networks First Report and Order*, 15 FCC Rcd at 23031 ¶ 106.

¹⁸⁰ 47 U.S.C. § 303(r); *Motion Picture Ass'n v. FCC*, 309 F.3d 796, 806 (D.C. Cir. 2002) (ruling that sections 4(i) and 303(r) are similar to "necessary and proper clauses" and are not themselves the sources of delegated authority).

¹⁸¹ *Competitive Networks First Report and Order*, 15 FCC Rcd at 23031 ¶ 106.

¹⁸² "A statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous No clause[,] sentence or word shall be construed as superfluous, void or insignificant if the construction can be found which will give force to and preserve all the words of the statute." Norman J. Singer, *Statutes and Statutory Construction* § 46:06 (6th ed. 2000) [hereinafter *Singer Statutory Construction*].

B. The FCC May Not Rely on Its Ancillary Jurisdiction to Regulate the Installation of Wi-Fi Antennas

The ancillary jurisdiction doctrine also fails to provide the FCC with the authority to extend the OTARD rule to the transmission and reception of fixed wireless signals. The FCC may exercise ancillary jurisdiction only if (1) its general grant of jurisdiction under Title I of the Communications Act covers the regulated subject, and (2) the regulations are reasonably ancillary to the effective performance of its statutorily mandated responsibilities.¹⁸³ Although the FCC invoked numerous statutory provisions to justify its claim of general jurisdiction,¹⁸⁴ including some combination of sections 1, 706, 201(b), 202(a), and 205(a) of the Communications Act of 1934, as amended, ("Communications Act") with either section 4(i) or 303(r) of the Communications Act, these provisions are an inadequate basis for its attempt to regulate the installation of Wi-Fi antennas on leased property.

Section 1 of the Communications Act does not provide the FCC with general jurisdiction over the installation of fixed wireless antennas on leased property. In the *First Report and Order*, the FCC attempted to justify the extension of the OTARD rule to fixed wireless services as part of its section 1 authority to "regulat[e] interstate and foreign commerce in communications by wire and radio"¹⁸⁵ The FCC asserted that section 1 authorized the extension of the OTARD rule to fixed wireless antennas because the extension would "facilitat[e] efficient deployment of competitive communications services."¹⁸⁶

¹⁸³ *American Library Ass'n v. FCC*, 406 F.3d 689, 700 (D.C. Cir. 2005).

¹⁸⁴ *Competitive Networks First Report and Order*, 15 FCC Rcd at 23028-23035 ¶ 101-116.

¹⁸⁵ *Id.* at 23029 ¶ 102 (quoting 47 U.S.C. § 151).

¹⁸⁶ *Id.*

This expansive interpretation conflicts with judicial decisions circumscribing the FCC's regulatory authority under section 1. Courts have repeatedly held that section 1 grants the FCC jurisdiction only over the actual transmission or reception of wire or radio communications.¹⁸⁷ For example, in *American Library Association v. FCC*, the D.C. Circuit reversed and vacated the broadcast flag rule after finding that the FCC lacked jurisdiction under Title I to require digital television receivers to include technology allowing them to recognize the broadcast flag.¹⁸⁸ Although the FCC had claimed that the definition of "radio communication" authorized its jurisdiction over television receivers because they are the apparatus for the receipt of radio communications, the court found that this definition limits the FCC's jurisdiction "to 'apparatus' that are 'incidental to . . . transmission.'"¹⁸⁹ Based on this definition, the court held that "at most, the Commission only has general authority under Title I to regulate apparatus used for the receipt of radio or wire communication *while those apparatus are engaged in communication*."¹⁹⁰ In other words, without express statutory authorization, the FCC has the authority to regulate Wi-Fi antennas only to the extent they are actively transmitting or receiving communications.

The amended OTARD rule exceeds the FCC's ancillary jurisdiction because it requires landlords to permit their tenants to install fixed wireless antennas on leased property, in this case premises owned by a governmental entity. As an initial matter, the FCC should not assert

¹⁸⁷ *American Library Ass'n*, 406 F.3d at 705; *Motion Picture Ass'n*, 309 F.3d at 804 (holding that the FCC had no authority under Title I to promulgate regulations that significantly implicated program *content*, as opposed to regulations that govern wire and radio *transmissions*); *Illinois Citizens Committee for Broadcasting v. FCC*, 467 F.2d 1397, 1399-1400 (7th Cir. 1972) (holding that the FCC may not lawfully exercise jurisdiction over an activity that does not constitute communication by wire or radio simply because the activity "substantially affects communications").

¹⁸⁸ *American Library Ass'n*, 406 F.3d at 691, 705, 708.

¹⁸⁹ *Id.* at 703.

¹⁹⁰ *Id.* at 704 (emphasis added).

jurisdiction over entities, such as landlords, that are not engaged in "communication by wire or radio," without express authorization from Congress. The FCC also should not assert jurisdiction over the installation of fixed wireless antennas. The act of installing antennas does not constitute "communication by wire or radio" under section 1 because it occurs prior to the transmission or reception of any radio signal. Because fixed wireless antennas are not actively transmitting or receiving "communications by wire or radio" at the time of installation, the FCC plainly exceeded the scope of its general jurisdictional grant under Title I in requiring landlords to permit the installation of such antennas on leased property. Finally, as mentioned above, if section 1 granted the FCC jurisdiction to regulate the installation of antennas, Congress would not have delegated similar authority to the FCC under section 207 of the Telecommunications Act of 1996.

Section 706 also fails to provide the FCC with the general jurisdiction to extend the OTARD rule to the installation of antennas used to provide fixed wireless signals.¹⁹¹ Under section 706, the FCC

shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability . . . by utilizing . . . price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, and other regulating methods that remove barriers to infrastructure investment."¹⁹²

The list of available methods to encourage deployment indicates that this provision applies in the common carrier context. In particular, price cap regulation, regulatory forbearance, and measures that promote competition in the local telecommunications market are all associated

¹⁹¹ *Competitive Networks First Report and Order*, 15 FCC Rcd at 23030 ¶ 103 (asserting jurisdiction under section 706 over "antennas used for the transmission or reception of fixed wireless signals").

¹⁹² 47 U.S.C. § 157 nt.

with the regulation of common carriers under Title II. Although the phrase "other regulating methods" is a more general phrase, basic principles of statutory interpretation require the FCC to interpret this phrase in light of the other specific examples and, thus, limit its application to the reception of common carrier signals.¹⁹³

Finally, the FCC lacks general jurisdiction over the installation of Wi-Fi antennas under sections 201(b), 202(a), and 205(a) of the Communications Act.¹⁹⁴ As the FCC explained in the *First Report and Order*, "[t]hese statutory provisions are intended to ensure that the rates, terms, and conditions for the provision of common carrier service are just, fair, and reasonable, and that there is no unjust or unreasonable discrimination in the provision of such service."¹⁹⁵ Because these provisions address the regulation of common carrier services, they provide no basis for the FCC's exercise of jurisdiction over the installation of Wi-Fi antennas for the provision of information services.

VIII. THE LEASE AGREEMENT DOES NOT AUTHORIZE CONTINENTAL TO INSTALL AND USE A WI-FI ANTENNA

Continental must comply with the non-interference and TAA requirements with respect to the installation and use of a Wi-Fi antenna. Although Continental asserts that "notwithstanding the filing of its Petition under the provisions of OTARD, Continental reserves its rights under the Lease and believes that it had the right to install and use its free wireless communications services," the referenced provisions offer no support for this proposition.

¹⁹³ "Where general words follow specific words in a statutory enumeration, the general words are construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words." *Singer Statutory Construction* § 47:17.

¹⁹⁴ 47 U.S.C. §§ 201(b), 202(a), 205(a).

¹⁹⁵ *Competitive Networks First Report and Order*, 15 FCC Rcd at 23030 ¶ 104 (citing 47 U.S.C. §§ 201(b), 202(a), 205(a)).

- Section 7.1(a)(iv). Although this provision permits "the conduct of operations, communications, reservations, and administrative office functions and activities in connection with air transportation performed by Tenant,"¹⁹⁶ it provides no authorization for the installation of a Wi-Fi antenna or other communications equipment in the Presidents Club. As mentioned above, sections 9.4, 9.8, and 10.3, among others, govern the installation of communications equipment.
- Section 7.1(a)(xi). This section refers to "the installation, operation, and maintenance of telecommunications equipment customarily used in air transportation operations, subject to approval under the TAA Process."¹⁹⁷ While this provision covers "telecommunications equipment," the provision of high-speed Internet access is not "telecommunications." Even if Continental were to use the Wi-Fi antenna for telecommunications, this provision still requires "approval under the TAA Process."
- Sections 7.2(b) and (c). Although these sections prohibit the sale of goods, they do not support an inference that the sale or provisions of services is permissible. The preliminary language of section 7.2 states that "Tenant shall not use the Premises for any use not specifically granted herein without the prior written approval of the Authority" and that "[p]rohibited uses are expressly agreed to include, but not be limited to," those listed in subsections (b) and (c).¹⁹⁸ Thus, the absence of any particular activity from the list is not evidence of its permissibility.
- Section 10.1(d). Section 10.1(d) merely states that Massport has no *obligation* to provide telephone or data communication services to the Presidents Club.¹⁹⁹ Continental may still purchase high-speed Internet access service from its current Internet service provider, Fiberlink, through the central Wi-Fi antenna system.
- Section 19.2. While this section states that "Tenant shall peacefully have and enjoy the Premises and the rights and privileges granted by this Lease,"²⁰⁰ it does not create any additional rights or privileges.

Thus, these provisions create no independent right for Continental to install and use a Wi-Fi antenna without complying with the non-interference and TAA requirements of the Lease Agreement.

¹⁹⁶ *Lease Agreement* § 7.1(a)(iv), attached as Exhibit A.

¹⁹⁷ *Id.* § 7.1(a)(xi).

¹⁹⁸ *Id.* § 7.2.

¹⁹⁹ *Id.* § 10.1.

²⁰⁰ *Id.* § 19.2.

WHEREFORE, THE PREMISES CONSIDERED, Massport respectfully requests that the FCC consider these Comments and proceed in a manner consistent with the views expressed herein.

Respectfully submitted,

THE MASSACHUSETTS PORT AUTHORITY

By: 
Christine M. Gill
Keith A. McCrickard
McDERMOTT WILL & EMERY LLP
600 Thirteenth Street, N.W.
Washington, D.C. 20005-3096
202.756.8000

David S. Mackey
Deborah Lau Kee
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
617.568.3131

Its Attorneys

Dated: September 28, 2005

CERTIFICATE OF SERVICE

I, Christine Biso, do hereby certify that on this 28th day of September 2005, a copy of the foregoing "Comments Of The Massachusetts Port Authority" was sent by first-class mail, postage prepaid, except as otherwise noted, to the following:

Marlene H. Dortch (Via ECFS)
Office of the Secretary
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

James D. Schlichting (Via E-mail)
Deputy Chief
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Bruce A. Romano (Via E-mail)
Associate Chief (Legal)
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Gary Thayer (Via E-mail)
Office of Engineering and Technology
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Donna J. Katos
Managing Attorney-Litigation
Thomas Newton Bolling
Senior Attorney-Regulatory
Continental Airlines, Inc.
1600 Smith Street-HQSLG
Houston, TX 77002

Henry M. Rivera
Vinson & Elkins, LLP
The Willard Office Building
1455 Pennsylvania Avenue, NW
Washington, DC 20004-1008
Counsel for Continental Airlines, Inc.

/s/Christine Biso
Christine Biso